

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
 (Print)

INTEGRITY INTERVIEW GUIDE

The information collected in this form is personal.

The Canada Border Services Agency (CBSA) is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods into Canada.

To fulfill this mission, employees of the CBSA must conduct themselves with honesty, integrity and trustworthiness. It is imperative, therefore, that the CBSA carefully assess the integrity of new applicants and current employees. To facilitate such an assessment, the CBSA has developed the following Integrity Interview Guide.

Applicant Surname	Applicant Given Name (s)
Mailing Address (Street address, city, province, postal code)	Telephone No.1
E-Mail Address	Telephone No. 2

FOR OFFICE USE ONLY

Form #		Applicant ID No.
Name of Interviewer	Signature	Date of interview conducted

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
 (Print)

NOTICE REGARDING THE COLLECTION AND USE OF PERSONAL INFORMATION

The information you provide in this document is collected under the authority of the **Financial Administration Act sections 7(1), 11.1(1) and 12(1) (e), Sections 5 and 11** of the **Canada Border Services Agency Act, Section 31** of the **Public Service Employment Act and the Policy on Government Security**. It is collected for the purposes of providing a security screening assessment, for the reliability status, security clearance or site access of individuals working or applying to work through appointment, assignment or contract at the Canada Border Services Agency. The information may be disclosed to the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) as service providers in accordance with the **Policy on Government Security**. The security screening status may be shared within the Canada Border Services Agency to update individual's personnel file. Information may also be shared with entities outside the Federal Government, including credit bureaus for the purposes of conducting reliability personnel security screening checks, conducting database checks, audit, statistical, periodic data matching and to assess an individual's loyalty and reliability as it relates to loyalty. The information may be used by accredited domestic law enforcement agencies in the administration or enforcement of the law and in the detection, prevention or suppression of a crime.

The information provided in this Integrity Interview will be retained by the CBSA for a minimum of two years and will be used to determine your suitability and reliability, and to conduct a security assessment for any other position within the CBSA to which you may apply. This may result in your disqualification from any previous processes you have applied for.

Individuals have the right of access to, the protection and correction of their personal information under the **Privacy Act**. The information collected is described under the **Personnel Security Screening Program Personal Information Bank CBSA PPU 1108** which is detailed at www.infosource.gc.ca.

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

NOTICE REGARDING THE INTEGRITY INTERVIEW GUIDE

You may withdraw from the application process at any time. You may refuse to provide answers to any or all of the questions from the Integrity Interview, however, such a refusal may result in your disqualification from the recruitment process.

You should answer the questions accurately, completely, thoroughly, and honestly to the best of your knowledge and belief.

Affirmative responses to questions from the Integrity Interview do not necessarily mean that you will be disqualified from the recruitment process. The Integrity Interview is one of a number of tools that is used to globally assess your honesty, trustworthiness, and integrity.

You are **not required** to provide any information that relates to a conviction for which a pardon has been received or a conviction that was processed pursuant to the *Young Offenders Act* (R.S.C. 1985, c. Y-1, now repealed) or the *Youth Criminal Justice Act* (S.C., 2002, c.1).

Should there be a change in circumstances, which would require that you amend any of the responses provided in the Integrity Interview, you should contact the Personnel Security and Professional Standards Division of the CBSA at 343-291-7684.

Deceit, dishonesty, or non-disclosure in any part of the application process is likely to result in your disqualification from the recruitment process and/or any future employment with the CBSA.

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

**NOTICE REGARDING MISCONDUCT, CRIMINAL OFFENCES
AND RISK TO THE SAFETY OF OTHERS**

The information you provide during the Integrity Interview is collected by the CBSA for the purposes of an employment application, and security screening. All answers which reveal criminal activity may be disclosed to the RCMP and CSIS as part of the security screening process.

If you declare during the Integrity Interview to having committed one or a number of criminal offence(s), for which a pardon was not obtained, be advised that the information may be disclosed to entities with lawful authority to collect such information (e.g. police of jurisdiction or child protection agency).

If, in light of the information provided throughout the screening process, you are deemed to pose a threat to others, be advised that the information may be disclosed to entities with lawful authority to collect such information (e.g. police of jurisdiction).

You are also advised that such disclosures could lead to incident reports being entered into police databases, which could impact future employment or volunteering opportunities, or other activities that require security screening (e.g. employment with schools, banks, etc.).

Such disclosures could also lead to an investigation, arrest, charge(s), criminal prosecution, conviction, and, ultimately, imposition of a sentence.

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
 (Print)

DECLARATION, ACKNOWLEDGMENT, AND CONSENT

Should you have any questions seek clarification from the interviewer before proceeding with the Integrity Interview.

Please ensure that you initial each of the following statements in the space provided:

	Applicant Initials
I, the undersigned, have read and understand the information and notices on Pages 1, 2, 3 and 4 of this Integrity Interview Guide	
I declare that I will provide, in this Integrity Interview, information that is up-to-date, accurate, complete and honest, to the best of my knowledge and belief.	
I understand that there is a possibility that I may amend my answer(s) to any question(s) in the Integrity Interview by contacting the CBSA Personnel Security and Professional Standards Division.	
I understand that I do not have to provide any information in this Integrity Interview that relates to a conviction for which a pardon has been received, or a conviction that was processed pursuant to the <i>Young Offenders Act</i> or the <i>Youth Criminal Justice Act</i> .	
I understand that the information provided in this Integrity Interview may affect my possibilities for any other employment with, or at, the CBSA within the next two (2) years, and/or, where applicable, may affect my current employment with, or work at, the CBSA.	
I understand that if I admit to having committed one or a number of criminal offence(s), during the Integrity Interview, actions could be taken which could lead, ultimately, to the imposition of a sentence.	
I consent to my personal information being collected, used, and disclosed for the purposes identified on the foregoing Pages 2,3,4 and ,5 of the Integrity Interview Guide	
I consent to my personal information being used for security screening pursuant to the Treasury Board Policy on Government Security http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578 .	

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
 (Print)

"I, the undersigned, do consent to the disclosure of the preceding information including my photograph for its subsequent verification and/or use in an investigation for the purpose of providing a security screening assessment. By consenting to the above, I acknowledge that the verification and/or use in an investigation of the preceding information may also occur when the reliability status, security clearance or site access are updated or otherwise reviewed for cause under the Policy on Government Security.

My consent will remain valid until such time as any such reliability status, security clearance or site access clearance is no longer a requirement for my continued employment with the CBSA, or any successor thereto, my employment is terminated, I am deployed to a position with another employer within the Government of Canada, or I revoke my consent, in writing, to the Director General, Security and Professional Standards of the CBSA."

_____ Name of Applicant (print)	
_____ Signature of Applicant	_____ Date

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

SECTION A - Driving History

1. Have you ever applied for a driver's licence and been denied or has your driver's licence ever been restricted, suspended or revoked for any reason, other than a medical reason?

☐ Yes ☐ No

If yes, explain:

2. Do you have any outstanding motor vehicle/driving violation(s) and/or unpaid traffic tickets, including parking tickets?

☐ Yes ☐ No

If yes, explain:

SECTION B – Alcohol/Drugs

3. Do you consume alcohol?

☐ Yes ☐ No

If yes, what is your consumption like? Please explain (for example: are you talkative or secretive? Do you maintain or lose control? Do you drink alone or with others? Where do you drink – home, bar, other?)

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

4. Have you ever purchased or supplied alcohol for minors?

☐ Yes ☐ No

If yes, explain:

5. Have you ever been charged with or convicted of operating a motorized vehicle or vessel while under the influence of alcohol and/or illegal drugs?

☐ Yes ☐ No

If yes, explain:

6. Have you been treated or sought treatment or counselling for a substance (e.g. drugs, alcohol) abuse problem, within the past three years?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

7. Have you used any illegal/illicit drugs, within the past three years?

☐ Yes ☐ No

If yes, provide the requested information for each drug and explain the circumstances of use in the chart below:

Drug	Method and Frequency of Use	Approximate dates of use (first time, last time)	Circumstances/ Motives for use	Means to obtain drugs	Financial outlay (How much do/did you spend on drugs on a monthly basis?)
Acid/LSD					
Bath Salt					
Catha Edulis (Khat)					
Cocaine					
Crack					
Crystal Meth					
Date Rape (DMX, GHB, Rohyphonol)					
Ecstasy					
Hash/Hash Oil					
Heroin					
Inhalants (glue, gasoline, paint)					
Ketamine					
Marijuana					
Mescaline					
Methamphetamine					
Mushrooms					
PCP					
Steroids					
Other (specify)					

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

8. Have you ever been involved in, investigated, charged with or convicted of selling any illegal or prescription/non-prescription drugs?

☐ Yes ☐ No

If yes, explain:

9. Have you ever been involved in, investigated, charged with or convicted of growing, producing or harvesting illegal drugs and/or, importing, exporting or mailing any illegal or prescription drugs?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

10. Have you misused or been dependent upon prescription drugs, within the past three years?

☐ Yes ☐ No

If yes, provide information for each drug and explain the circumstances of use in the chart below:

Drug	Method and Frequency of Use	Approximate dates of use (first time, last time)	Circumstances/ Motives for use	Financial outlay (How much do/did you spend on drugs on a monthly basis?)
Antihistamines				
Dilaudid				
Methadone				
Oxycodine				
Oxycontin				
Percocet				
Percoden				
Prozac				
Ritalin				
Valium				
Zanax				
Other (specify):				

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

11. Have you ever been involved in, investigated, charged with or convicted of any offence involving trafficking, importing and/or exporting drugs?

☐ Yes ☐ No

If yes, explain:

12. Have you knowingly associated with anyone who has been involved in, investigated, charged with or convicted of any criminal acts involving illegal drugs (family, friends, etc.), within the past three years?

☐ Yes ☐ No

If yes, explain:

13. Have you posted bail or bond for anyone who has been arrested (family, friends, etc.), with the past three years?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

SECTION C - Financial

NOTE: Provide any requested currency amounts in Canadian dollars, if possible.

14. What has your financial situation been like, within the past three years (CRA, Liens, personal bankruptcies or any other major changes)?

☐ Yes ☐ No

If yes, explain:

15. Have you gambled (including lottery, casinos, online gaming, scratch tickets, etc.), within the past three years?

☐ Yes ☐ No

If yes, how often and explain:

16. Do you presently owe any gambling debts? If yes, are you able to pay your gambling debts?

☐ Yes ☐ No

If yes, specify:

Amount (In Canadian \$)	Organization/ Person Debt Owed to	Date incurred

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

17. Are you able to pay any other financial debts?

☐ Yes ☐ No

If no, explain:

SECTION D - Security

18. Have you ever been involved in, investigated, charged with or convicted of providing fraudulent or misleading information regarding yourself? Other people? Or persons seeking entry into Canada?

☐ Yes ☐ No

If yes, explain:

19. Have you ever been involved in, investigated, charged with or convicted of possessing false/fraudulent identification?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____

(Print)

20. Do you possess multiple citizenships or were you ever a citizen of another country other than Canada?

☐ Yes ☐ No

If yes, identify type of citizenship and country below:

☐ Multiple ☐ Former Country: _____

21. Do you have any foreign property, business connections, or financial interests?

☐ Yes ☐ No

If yes, explain:

22. Is there anything in your past or present that could make you susceptible to be subjected to blackmail/attempted blackmail, coercion or corruption?

☐ Yes ☐ No

If yes, explain:

SECTION E - Use of Force

23. Have you ever been involved in, investigated, charged with or convicted of committing acts or threats of violence?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

24. Have you ever been involved in, investigated, charged with or convicted of any offence involving the misuse, possession or storage of a firearm or other weapon?

☐ Yes ☐ No

If yes, explain:

25. Have you ever been involved in, investigated, charged with or convicted of pointing a weapon, or an item intended to be used as a weapon?

☐ Yes ☐ No

If yes, explain:

26. Would you consider yourself a person who has difficulties managing anger?

☐ Yes ☐ No

If yes, explain:

27. Have you ever been refused a firearms permit/licence or had a firearm permit/licence revoked?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

SECTION F - Unlawful Sexual Activity

28. Have you ever been involved in, investigated, charged with or convicted of travelling outside of Canada for the purpose of engaging in illegal sexual activity?

☐ Yes ☐ No

If yes, explain:

29. Have you ever been involved in the illegal sex trade and/or have you ever been charged with or convicted of soliciting the services of a prostitute?

☐ Yes ☐ No

If yes, explain:

30. Have you ever been involved in, investigated, charged with or convicted of engaging in sexual activities with someone who was under the age of consent ?

☐ Yes ☐ No

If yes, explain:

31. Have you ever been involved in, investigated, charged with or convicted of having sex with someone against his/her will or without his/her consent (includes persons unable to give permission due to a medical condition, mental health condition, alcohol, drugs, or other reasons)?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

32. Have you ever been involved in, investigated, charged with or convicted of viewing, possessing, storing, producing or downloading images of child pornography, bestiality and/or other illegal subject matter on the Internet?

☐ Yes ☐ No

If yes, explain:

SECTION G - Involvement with Law Enforcement

33. Have you ever been put on probation, had a court order issued against you or were under court supervision (includes search warrant, arrest warrant, peace bond, restraining order(s), protection order or restitution order)?

☐ Yes ☐ No

If yes, explain:

34. Have you ever been involved in, investigated, charged with or convicted of any criminal offence in Canada, USA or in any other country?

☐ Yes ☐ No

If yes, explain:

35. Have you ever associated in any way with people involved in organized crime, criminal activities, or terrorist activities?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

36. Have you ever been questioned or investigated by the CBSA (Immigration, Customs, and/or Canadian Food Inspection Agency), US Customs and Border Protection, US Border Patrol, any police agency or any Government Department/Agency as a complainant, a witness or a suspect?

☐ Yes ☐ No

If yes, explain:

37. Have you ever been involved in, investigated, charged with or convicted of illegally importing or exporting goods of any kind from or into any country including Canada?

☐ Yes ☐ No

If yes, explain:

SECTION H - Computers and Technology

38. Have you ever been involved in, investigated, charged with or convicted of using a phone, a computer or the Internet for illegal or nuisance purposes and/or attempted to gain unauthorized access into any computer system (i.e. business, private, law enforcement, Canadian or foreign government systems)?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

39. Have you ever been involved in, investigated, charged with or convicted of committing credit card/bank card fraud, identity theft, or any other form of false pretense?

☐ Yes ☐ No

If yes, explain:

SECTION I - Employment

40. Did you omit any prior places of employment from your security application (within the past ten years)?

☐ Yes ☐ No

If yes, explain:

41. Have you ever been an employee of and/or have you ever been refused employment with the Government of Canada, the military, any police service, and/or any intelligence service (includes the CBSA, the Department of National Defence, the RCMP and the Canadian Security Intelligence Service)?

☐ Yes ☐ No

If yes, explain:

42. Have you ever had your employment terminated, suspended and/or have you ever been asked to resign from any previous employment?

☐ Yes ☐ No

If yes, explain:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

SECTION J – Affiliations

43. Within the past 10 years, have you been employed by a government or an organization (Canadian or foreign) in a security-related capacity?

☐ Yes ☐ No

If yes, explain and provide details on the group/organization:

44. Have you ever held a position of authority in any government, or judiciary or a political party outside of Canada?

☐ Yes ☐ No

If yes, explain and provide details on the group/organization and the position you held and/or your relationship with them:

45. Have you ever been involved with a military, militia, civil defence unit or policing organization?

☐ Yes ☐ No

If yes, explain and provide details on the group/organization.

46. Have you been a member or associated with any group or organization which has engaged in or advocated violence, hate propaganda, or which has been associated with criminal activity at any time?

☐ Yes ☐ No

If yes, explain and provide details on the group/organization:

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____

(Print)

47. Have you ever sponsored anyone from another country to come to Canada?

☐ Yes ☐ No

If yes:

a) Who have you sponsored? Please provide details regarding the principal applicant that you are currently or have sponsored in the past, including their country of origin as well as the country they are being or were sponsored from, the date of sponsorship, their full name(s) and date(s) of birth as well as the current address.

b) What form of sponsorship did you use (i.e. family, spouse or common-law, employment, etc.)?

c) Indicate the nature of your relationship to the principal applicant?

d) Indicate the principal applicant's current status in Canada?

e) Indicate if you are aware of the principal applicant's activities and the relevant details of those activities, including any criminal activity, any associations with any group or organizations which have engaged in or advocated violence, or which have been associated with criminal activity at any time along with the name and type of activity / organization.

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

This Integrity Interview is not complete until you have read, understood, signed, and dated the **Final Declaration, Acknowledgment, and Consent**.

Final Declaration, Acknowledgment, and Consent of: _____
Name of Applicant (print)

I, the undersigned, hereby declare that the information I have provided in this Integrity Interview (referred to on this page as the preceding information) is up to date, accurate, complete, and honest, to the best of my knowledge and belief.

I further acknowledge that the verification and/or use of the preceding information may also occur when my reliability status, security clearance or site access - if issued - are updated or otherwise reviewed for cause under the Policy on Government Security.

If I provided statements containing criminal admissions, I acknowledge that the CBSA may use and/or disclose such information for a law enforcement or public safety purpose as described under the "Notice Regarding Misconduct, Criminal Offences and Risk to the Safety of Others" on Page 4 of this Integrity Interview Guide

By my signature below, I declare that I have read and understand how the preceding information will be managed and I hereby consent to the use and disclosure of my personal information as described herein above.

Signature of Applicant

Date

Security Volume – Directive on CBSA Personnel Security Screening

Table of Contents

- Effective Date
- Application
- Context
- Definitions
- Policy Statement
 - Objective
 - Expected Results
- Roles and Responsibilities
 - President
 - Departmental Security Officer (DSO)
 - Personnel Security Screening Section
 - Regional/Headquarters Security Manager
 - Human Resources
 - CBSA Managers
 - Employees
- Consequences
- References
- Enquiries

1. Effective Date

1.1. This directive takes effect on January 6, 2015.

2. Application

2.1. This directive applies to:

- All individuals who will have access to Canada Border Services Agency (CBSA) information and assets; and
- All applicants to and employees (permanent, term, casual, part-time) of the CBSA, contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students.

3. Context

The Government of Canada's Policy on Government Security (PGS) requires the CBSA to ensure that all individuals who will have access to government information and assets are

security screened at the appropriate level before the commencement of their duties and are treated in a fair and unbiased manner. This directive describes how the CBSA will manage Personnel Security in accordance with the PGS.

Security begins by establishing trust in interactions between government and Canadians and within government. Within government, there is a need to ensure that those having access to government information, assets and services are trustworthy, reliable and loyal. The CBSA's Personnel Security Program has been established to support these requirements.

The Personnel Security Program limits access to information and assets to those individuals with a need to know. It ensures that an individual is appropriately screened based on the information and access required for the performance of his or her job. Effective Personnel Security management enables the CBSA:

- To ensure that individuals with access to government information/assets and/or privileged access to critical systems are reliable and trustworthy;
- To ensure the individual's loyalty to Canada in order to protect itself from foreign intelligence gathering and terrorism; and
- To prevent malicious activity and unauthorized disclosure of protected and classified information or damage affected on critical systems by a disaffected individual in a position of trust.

In recognition of the CBSA's role in law enforcement, national security and public safety and the demonstrated risk exposure to incidents of corruption, fraud and criminal interference, the Agency received Treasury Board approval to implement additional Personnel Security screening tools to augment the baseline screening requirements.

4. Definitions

Specific definitions drawn from authoritative sources are included in the [Glossary of Security Terminology](#).

5. Policy Statement

5.1. Objective

The objective of this directive is to ensure that the CBSA provides the appropriate access to Government of Canada (GoC) information and assets to personnel who have been deemed trustworthy and loyal in accordance with the Policy on Government Security (PGS).

5.2. Expected Results

- Compliance with the PGS;
- Employees understand their responsibilities regarding the security of Government information and assets;

- Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;
- Interoperability and information exchange with other GoC Personnel Security Departments and Agencies;
- Mechanisms and resources are in place to ensure effective and efficient management of Personnel Security at the CBSA;
- Individuals with access to Agency information and assets have integrity, are reliable, honest and trustworthy;
- The vulnerability to influence by criminal elements is reduced;
- The potential security risks to sensitive information and assets are minimized; and
- The protection of program integrity.

6. Roles and Responsibilities

6.1. President

The President of the CBSA is responsible for effectively managing security activities within the CBSA and contributing to effective government-wide security management. The President is responsible for:

- Ensuring the CBSA's compliance to the PGS and other related policy instruments and legislation;
- Approving the CBSA's Departmental Security Plan and establishing a security program for the coordination and management of overall security activities, including Personnel Security;
- Appointing a Departmental Security Officer to manage the departmental security program;
- Ensuring that managers at all levels integrate Personnel Security requirements into plans, programs, activities and services;
- Denying, suspending or revoking a Reliability Status in the case of just cause;
- Denying, suspending or revoking a Security Clearance in the case of just cause; and
- Ensuring that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence, they are investigated, acted upon and reported to the appropriate authorities.

6.2. Departmental Security Officer (DSO)

The Departmental Security Officer (DSO) is responsible for the management of CBSA's Security Program and has the following responsibilities with regard to Personnel Security:

- Developing, implementing, monitoring and maintaining a Departmental Security Plan which incorporates Personnel Security;
- Ensuring a coordinated approach to all aspects of CBSA Security: Personnel Security, IM, COMSEC, Contract and Physical Security;

- Ensuring that accountabilities, delegations, reporting relationships, and roles and responsibilities of CBSA employees with security responsibilities are defined, documented and communicated to relevant persons;
- Granting a Reliability Status and Security Clearance;
- Delegating the granting of a Reliability Status and Security Clearance by the DSO;
- Giving advice and making recommendations to the President in cases of denial, suspension or revocation of a Security Clearance; and
- Where just cause exists:
 - Denying, revoking or suspending a Reliability Status and informing the manager or Director.

6.3. Personnel Security Screening Section

The Personnel Security Screening Section (PSSS) is responsible for the coordination of all functions related to the technical and operational aspects of Personnel Security, specifically:

- Ensuring that all individuals who require access to Protected/Classified information or/and assets or/and privileged access to critical systems, have been granted the required CBSA approved Security level **prior** to the start of any assignment, appointment or secondment as a Reliability status or a Security Clearance is a condition of employment at the CBSA.
 - Reliability Status is required if access to Protected (A, B or C) information is a requirement of the work duties.
 - A Secret Security Clearance is required if access to Classified information is a requirement of the work duties. It is also required when privileged access to critical systems is needed to perform work duties.
 - Top Secret clearance is required if access to Classified information is a requirement of the work duties and there is a need to know to access information classified as Top Secret.
- Maintaining a functional or direct reporting relationship with the DSO to ensure departmental security activities are coordinated and integrated;
- Selecting, implementing and maintaining security controls related to the Personnel Security;
- Determining the security requirements of each position based on the sensitivity of the information, assets and privileged access to critical systems to which the incumbent has access;
- Advising managers and/or Human Resources (HR) of the status of the security assessment;
- Processing requests for personnel security screenings, including criminal record name checks, credit checks, verification of databases with Customs and Immigration information, Law Enforcement Record Checks, conducting integrity interviews, and conducting loyalty assessments ;
- Advising HR, Regional Security or HQ Security in writing of the candidate's personnel security screening results;

- Ensuring that all employees / contractors have received the official briefing by the employee's manager and have signed the Security Screening Certificate and Briefing Form;
- Maintaining employee personnel security screening files;
- Ensuring that Reliability Status and Security Clearances are updated, in accordance with the Security requirements of the position. The Security Officer will update:
 - a Reliability Status: every 10 years
 - a Secret clearance: every 10 years
 - a Top Secret clearance: every 5 years
- Conducting an update to the security screening of any employee who has been away from the workplace for over 1 year; and
- Performing reviews of screenings for cause and conducting investigations when required.

6.4. Regional/Headquarters Security Manager

Regional and Headquarters Security Managers are responsible for:

- Providing advice and guidance regarding the security screening process;
- Reviewing the completed personnel security screening forms for accuracy prior to forwarding it to the PSSS; and
- Ensuring that integrity interviews are conducted when required by PSSS.

6.5. Human Resources

Human Resources are responsible for:

- Verifying the following information for new employees:
 - Personal data (i.e. date of birth, address)
 - Education / professional qualifications
 - Employment history
 - Personal Character
- Initiating the Personnel Security Screening process; and
- Ensuring that no employee is hired/appointed/acting in a position without being security screened and granted his or her required CBSA Reliability Status or Security Clearance by the DSO.

6.6. CBSA Managers

Managers are responsible for:

Managers are responsible for ensuring an appropriate level of security for their programs and services. In designing programs and services, managers will work with departmental security specialists to effectively manage risk. Managers will be supported and assisted by the PSSS in order to fulfill the following responsibilities:

- Ensuring that security requirements are integrated into business planning, programs, services and other management activities;
- Ensuring employees apply effective security practices;
- Identifying the sensitivity of the information, assets and privileged access to critical systems for each position of their unit and informing the CBSA PSSS to obtain the proper Security requirement for the position;
- Ensuring that no individual is hired/appointed/acting or commences any work in a position without being screened and granted his or her required CBSA approved Security Level by the PSSS, including acting assignments;
- Controlling access to protected/classified information and assets to persons who have acquired the proper Security Clearance and who have a “need-to-know”; need-to-know means the need for someone to access and know information in order to perform his or her duties.
- When contracts are required, identifying any security requirements and ensuring that no temporary help, contractor or consultant is hired or commences any work without being screened and has been granted the appropriate CBSA approved security level as required in the contract or agreement;
- Reporting adverse information to the Security and Professional Standards Directorate (SPSD);
- Ensuring that a Security Briefing is provided to every employee upon hire; and
- Ensuring that employees take the Online Security Awareness Module within two weeks of joining the CBSA and repeating the module every two years thereafter.

6.7. Employees

Employees are responsible for:

- Safeguarding information and assets under their control whether working on CBSA premises or off-site;
- Applying security controls related to their area of responsibility to ensure that security requirements are part of their day-to-day processes, practices and program delivery;
- Reporting security incidents through the appropriate channels; and
- Informing their manager of any issues affecting their Reliability Status or Security Clearance:
 - Arrest or Criminal conviction;
 - Bankruptcy;
 - Single/cohabitating/marriage/divorce; and/or
 - If approached by someone criminal, a representative of a foreign government, a fringe interest group or a foreign national who is seeking information about CBSA or the activities of CBSA, which would compromise the national interest, or the integrity of the Agency.

7. Consequences

CBSA employees are held to high standards based on the nature of the work they do. There is a requirement for CBSA employees to have honesty, integrity and trustworthiness – the HIT

factor. CBSA employees who are found to have breached the HIT factor, CBSA Code of Conduct, the Policy on Government Security, the Values and Ethics Code or any other applicable CBSA or Government of Canada policies, standards or legislation, will be subject to disciplinary measures based on the seriousness of the misconduct and in accordance with the CBSA Discipline Policy. In some cases this may mean a review and possibly a revocation of the CBSA Reliability Status.

8. References

This directive is issued under section 7 of the Financial Administration Act and should be read in conjunction with:

- [The CBSA PerSec Standard](#)
- [Standard Operating Procedures for Security Requirement Checklist \(SRCL\)](#)
- [Policy on Government Security](#)
- [Directive on Identity Management](#)
- [Directive on Departmental Security Management](#)
- [Standard on Security Screening](#)
- [Operational Security Standard: Management of Information Technology Security \(MITS\)](#)
- [CBSA Code of Conduct](#)
- [Values and Ethics Code for the Public Sector](#)
- [Criminal Code of Canada](#)

9. Enquiries

For more information, please contact: [Security and Professional Standards Directorate](#)

Date modified:

2015-03-25

Security Volume – Standard for CBSA Personnel Security Screening

Table of Contents

- [Purpose](#)
- [Effective Date](#)
- [Application](#)
- [Context](#)
- [Definitions](#)
- [Authorities](#)
- [Objective](#)
- [Process](#)

- [Assessment of Background Checks](#)
- [Consequences](#)
- [Personnel Security Screening Service Standards](#)
- [References](#)
- [Enquiries](#)

Purpose

The purpose of this Standard is to ensure that in accordance with the Policy on Government Security (PGS), the Canada Border Services Agency (CBSA) security screens all individuals with access to government information and assets at the appropriate level before the commencement of their duties. The CBSA conducts its personnel security screening checks in accordance with the PGS – Personnel Security Standard, and additionally, conducts CBSA specific background checks at the Reliability Status level, which have been approved by the Treasury Board.

Effective Date

This Standard takes effect on January 6, 2015.

Application

The standard applies to:

- All individuals who will have access to Canada Border Services Agency (CBSA) information and assets; and
- All applicants to and employees (permanent, term, casual, part-time) of the CBSA, contract and private agency personnel and to individuals seconded or assigned to the CBSA, including students.

Context

Personnel Security Screening is a proactive management process that requires the examination of the honesty, integrity and trustworthiness (HIT factor) of all individuals working at the CBSA ^{Footnote 1} to protect the Agency's personnel, assets and information. It involves the use of various checks and assessments which are conducted as part of the Reliability Status screening process, which is the foundation for all personnel security screenings. The level of security screening required is dependent upon the security level of information and assets that will be accessed in the normal performance of assigned job duties or during the contracting process.

This process involves:

- Determining the type and level of screening required;
- Identifying the types of verifications required;

- Obtaining consent;
- Processing verifications and assessments;
- Evaluating results of verifications and assessments;
- Granting or denying a reliability status or security clearance;
- Making the appointment, awarding the contract or entering into a written collaborative agreement; and
- Providing a briefing to the screened individual.

Definitions

Specific definitions drawn from authoritative sources are included in the Glossary of Security Terminology.

Authorities

This Standard is issued under section 7 (1) and section 12 (1)(e) of the *Financial Administration Act*.

It is to be read in conjunction with:

- The appendices to this Standard
- The CBSA Security Volume, and specifically the Policy on Professional Standards Investigations

Objective

The objective of this standard is to ensure that the Agency can effectively meet the requirements set forth in its Personnel Security Screening Section (PSSS) to ensure that individuals are cleared to the appropriate level should they meet the screening criteria, which are:

- Determining the honesty, integrity, trustworthiness and reliability of individuals who will have access to government assets, information, networks and government facilities;
- Preventing malicious activity and unauthorized disclosure of Protected and Classified information by an individual in a position of trust;
- Ensuring the loyalty to Canada of individuals who will have access to Classified information and highly critical assets;
- Protecting itself from foreign intelligence gathering and terrorism, or from those who are engaged in other activities viewed as being threats to the security of Canada, as defined in Part II, 21 (2) of the *Canadian Security Intelligence Service (CSIS) Act*; and
- Denying access to government assets and information to individuals involved in criminal acts which are considered to pose an unacceptable risk to the Agency

Process

In addition to the baseline verifications of employment history, credit and criminal record checks, all individuals applying to the CBSA, as well as all employees of the CBSA undergoing a renewal or upgrade of their screening, will also undergo the following verifications:

- Law Enforcement Record Checks;
- Internal data base checks;
- Integrity Interviews for uniformed officers and case by case for others; and
- Other checks may be undertaken for cause on a case by case basis.

There are two types of Personnel Security Screenings: an assessment of reliability; and an assessment of loyalty and reliability related to loyalty. The types and levels of Personnel Security Screening which apply to the CBSA and are as follows:

CBSA Reliability Status indicates the successful completion of reliability checks; allows regular access to government assets with a need to know to protected information.

- Forms required for CBSA Reliability Status:
 - Personnel Screening, Consent and Authorization Form ([BSF697E \(PDF, 840 KB\)](#))
 - CBSA Consent Statement ([BSF684 \(PDF, 560 KB\)](#))

Note: [How to complete the Security Clearance Form TBS 330-23](#)

A Security Clearance, otherwise known as a Secret or Top Secret is a clearance granted to an individual who requires on a “need to know” basis, access to classified information, assets and/or restricted work sites.

- Forms required for a Security Clearance (in addition to the forms required for a CBSA Reliability Status):
 - Security Clearance Form ([TBS/SCT 330-60E](#))

Note: [How to complete the Security Clearance Form TBS 330-60](#)

Residency and Travel Outside of Canada Questionnaire: The questionnaire ([BSF 641E \(PDF, 1.54 MB\)](#)) is to be completed if an applicant or employee has been out of the country for 90 consecutive days or more within the last 5 years for Reliability Status and 10 years for Security Clearance:

Note: All armed officers who do not hold a valid Possession and Acquisition Licence (PAL) or who have not yet been screened through the CBSA personnel security screening process, will be screened through this process in advance of their normal renewal cycle.

New security screening forms are required for the processing of a new screening, renewal of an existing screening, an upgrade or any update to an existing security screening. This includes individuals who have a security screening from another government department.

Note: Any type of extended leave over 1 year would require new forms to be submitted for the processing of an update to an individual's existing security screening. New security screening forms may also be requested at any time for cause.

All completed forms required for the individual's specified level of screening need to be submitted to the nearest Regional Security Office for vetting and submission to the CBSA Personnel Security Screening Section for processing.

Assessment of Background Checks

Should adverse information become available through the various checks conducted through the CBSA PSSS, the adverse information shall be considered as per the PGS, with respect to:

- Its nature;
- Seriousness;
- Surrounding circumstances;
- Frequency;
- The willingness of participation;
- The individual's age at the time of the incident(s); and
- The degree of rehabilitation.

Other areas for assessment:

- The honesty, integrity and trustworthiness of the individual (HIT factor)
- Recognition of the seriousness of the misconduct by the employee;
- The aggravating and mitigating factors;
- The possibility this situation was error of judgement (intent/mens rea);
- Other relevant personal circumstances;
- The consequences in terms of injury/potential injury to the organization;
- How would a reasonable person placed in the same context interpret the facts;
- Is the organization ready to accept the level of risk this employee represents;
- Consider the balance of probabilities; and
- Seriousness of the misconduct.

Assessment of Drug Related Offences:

- An applicant may be rejected for:
 - The non-medical use of any illegal drug within the last three years;
 - A history of drug consumption within the last three years;
 - The non-medical use of any drug within the last three years , that was more than occasional or experimental use;
 - The non-medical use of any anabolic steroids, hormones or amphetamines for the purpose of enhancing athletic ability, within the last three years; and
 - Being associated with a person who illegally uses or sells drugs or illegal substances within the last three years or after application.

The severity of drug use can be defined as:

Experimental use

means that a person consumed a drug six times or less and subsequently terminated the use of any illegal drug.

Occasional use

means that a person accepts/takes a drug when offered, but does not go out of his/her way to procure it, nor attempt to ensure a regular supply. The occasional user consumes a drug less than once a month.

Regular use

means frequently using an illegal drug once a month or more.

Abuse

means the intentional use of any illegal drug or misuse of a prescription or non-prescription drug which within the last three years that has led to significant impairment or distress, including use in a hazardous fashion, continued use despite problems, or failure to fulfill major role obligations at work, school or in the family.

Dependent use

means a pattern or regular use of an illegal, prescription or non-prescription drug which indicates a physical or emotional need to experience its effects or to avoid the discomfort of its absence. It is associated with an inability to reduce the use of drugs, continued use despite negative consequences (e.g. legal, financial or family). A great deal of time is spent getting or using the drug and important social, occupational, or recreational activities are given up or reduced because of drug use.

All drug related offences will be reviewed on a case by case basis using the above criteria in the decision making process.

The presence of adverse information on a file does not necessarily mean that an individual's screening will be denied or revoked. Each file is reviewed based on its own merits and criteria and a global assessment is conducted, where all information gathered for personnel security screening purposes is evaluated.

Consequences

CBSA employees are held to high standards based on the nature of the work they do. There is a requirement for CBSA employees to have honesty, integrity and trustworthiness – the HIT factor. CBSA employees who are found to have breached the HIT factor, CBSA Code of Conduct, the Policy on Government Security or the Values and Ethics Code or any other applicable CBSA policies or standards, will be subject to disciplinary measures based on the seriousness of the misconduct and in accordance with the CBSA Discipline Policy. In some cases this may mean a review and possibly a revocation of the CBSA Reliability Status.

An individual who has been denied or revoked a Reliability Status may not re-apply until after a two year period has passed and the HIT factor has been met. This does not mean that the individual who is re-applying will necessarily be granted a screening but rather allows an

opportunity for them to re-submit an application to the CBSA. All re-applications will be reviewed on their own merits and criteria.

Personnel Security Screening Service Standards

- Reliability Status: 20 business days
- Secret Clearance: 60 business days
- Top Secret Clearance: 75 business days

References

- Policy on Government Security
- Standard on Security Screening

Enquiries

For further information, please contact: Security and Professional Standards Directorate

Or

For questions regarding the Personnel Security Screening Process, please contact your Regional / Headquarters Security Manager.

Annex 33 - Justification for the Questions in the Integrity Interview Guide

The information sought is directly related to the criteria identified for obtaining a reliability clearance status from the Canada Border Services Agency in accordance with the Policy on Government Security (2009). The respective criteria are the applicant's honesty, integrity and trustworthiness. These criteria are very important because the Canada Border Services Agency plays an enforcement role. Society holds people who have these types of positions or who work in law enforcement to a higher standard.

It is important to note that the main purpose of this questionnaire is to serve as a guide during security interviews to ensure that all applicants are evaluated uniformly, using the same criteria and without exceptions in terms of risk assessment. A section may not be delved into if the applicant confirms that it does not apply to him or her. One example, among others, would be drug use, and the same would apply to the section on bankruptcy, and so on.

Interviewers are trained to minimize the intrusiveness of the questions and to focus on the topics mentioned because they are aware and mindful of the applicant's right to privacy. Race, religion and sexual orientation will not be discussed because they have no bearing on risk assessment.

Interviewers must stick to security issues and not get sidetracked by psychological issues,

To that end, they must determine before asking for clarification whether the questions relate to the applicant's integrity, honesty and trustworthiness in terms of personnel security. If the answer is no, the questions cannot be asked.

The information gathered during the interview will be accessible only to the personnel security officer responsible for the applicant's file. The information will be used solely for the purpose of obtaining reliability status and a security clearance. Access to it will be on a need to know basis. None of the information will be shared internally in the Agency for purposes other than those for which it was collected.

There are ten separate sections in this guide for evaluating key components for an enforcement agency to prevent people who represent a risk to the Agency from being hired. The answers provided will be evaluated not only in terms of the topics explored, but in conjunction with the answers received in the other sections. The objective is to properly assess the risk the person could represent for the Agency, its employees, partners and clients.

Reference is made in the administrative component of the guide to the importance of the applicant fully grasping the purpose of the interview, his or her obligation to answer questions honestly and understanding the impact should he or she fail to do so.

Annex 34 - Integrity Interview Guide

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
 (Print)

INTEGRITY INTERVIEW GUIDE

The information collected in this form is personal.

The Canada Border Services Agency (CBSA) is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods into Canada.

To fulfill this mission, employees of the CBSA must conduct themselves with honesty, integrity and trustworthiness. It is imperative, therefore, that the CBSA carefully assess the integrity of new applicants and current employees. To facilitate such an assessment, the CBSA has developed the following Integrity Interview Guide.

Applicant Surname	Applicant Given Name (s)
Mailing Address (Street address, city, province, postal code)	Telephone No. 1
E-Mail Address	Telephone No. 2

FOR OFFICE USE ONLY

Form #		Applicant ID No.
Name of Interviewer	Signature	Date of interview conducted

Annex 34 - Integrity Interview Guide

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
 (Print)

NOTICE REGARDING THE COLLECTION AND USE OF PERSONAL INFORMATION

The information you provide in this document is collected under the authority of the **Financial Administration Act sections 7(1), 11.1(1) and 12(1) (e), Sections 5 and 11** of the **Canada Border Services Agency Act, Section 31** of the **Public Service Employment Act and the Policy on Government Security**. It is collected for the purposes of providing a security screening assessment, for the reliability status, security clearance or site access of individuals working or applying to work through appointment, assignment or contract at the Canada Border Services Agency. The information may be disclosed to the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) as service providers in accordance with the **Policy on Government Security**. The security screening status may be shared within the Canada Border Services Agency to update individual's personnel file. Information may also be shared with entities outside the Federal Government, including credit bureaus for the purposes of conducting reliability personnel security screening checks, conducting database checks, audit, statistical, periodic data matching and to assess an individual's loyalty and reliability as it relates to loyalty. The information may be used by accredited domestic law enforcement agencies in the administration or enforcement of the law and in the detection, prevention or suppression of a crime.

The information provided in this Integrity Interview will be retained by the CBSA for a minimum of two years and may be used to determine your suitability and reliability, and to conduct a security assessment for any other position within the CBSA to which you may apply. This may result in your disqualification from any previous processes you have applied for.

Individuals have the right of access to, the protection and correction of their personal information under the **Privacy Act**. The information collected is described under the **Personnel Security Screening Program Personal Information Bank CBSA PPU 1108** which is detailed at www.infosource.gc.ca.

Annex 34 - Integrity Interview Guide

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

NOTICE REGARDING THE INTEGRITY INTERVIEW GUIDE

You may withdraw from the application process at any time. You may refuse to provide answers to any or all of the questions from the Integrity Interview, however, such a refusal may result in your disqualification from the recruitment process.

You should answer the questions accurately, completely, thoroughly, and honestly to the best of your knowledge and belief.

Affirmative responses to questions from the Integrity Interview do not necessarily mean that you will be disqualified from the recruitment process. The Integrity Interview is one of a number of tools that is used to globally assess your honesty, trustworthiness, and integrity.

You are **not required** to provide any information that relates to a conviction for which a pardon has been received or a conviction that was processed pursuant to the *Young Offenders Act* (R.S.C. 1985, c. Y-1, now repealed) or the *Youth Criminal Justice Act* (S.C., 2002, c.1).

Should there be a change in circumstances, which would require that you amend any of the responses provided in the Integrity Interview, you should contact the Personnel Security and Professional Standards Division of the CBSA at 613-948-7576.

Deceit, dishonesty, or non-disclosure in any part of the application process is likely to result in your disqualification from the recruitment process and/or any future employment with the CBSA.

Annex 34 - Integrity Interview Guide

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

NOTICE REGARDING MISCONDUCT, CRIMINAL OFFENCES AND RISK TO THE SAFETY OF OTHERS

The information you provide during the Integrity Interview is collected by the CBSA for the purposes of an employment application, and security screening. All answers which reveal criminal activity may be disclosed to the RCMP and CSIS as part of the security screening process.

If you declare during the Integrity Interview to having committed one or a number of criminal offence(s), for which a pardon was not obtained, be advised that the information may be disclosed to entities with lawful authority to collect such information (e.g. police of jurisdiction or child protection agency).

If, in light of the information provided throughout the screening process, you are deemed to pose a threat to others, be advised that the information may be disclosed to entities with lawful authority to collect such information (e.g. police of jurisdiction).

You are also advised that such disclosures could lead to incident reports being entered into police databases, which could impact future employment or volunteering opportunities, or other activities that require security screening (e.g. employment with schools, banks, etc.).

Such disclosures could also lead to an investigation, arrest, charge(s), criminal prosecution, conviction, and, ultimately, imposition of a sentence.

Annex 34 - Integrity Interview Guide

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
 (Print)

DECLARATION, ACKNOWLEDGMENT, AND CONSENT

Should you have any questions seek clarification from the interviewer before proceeding with the Integrity Interview.

Please ensure that you initial each of the following statements in the space provided:

	Applicant Initials
I, the undersigned, have read and understand the information and notices on Pages 1, 2, 3 and 4 of this Integrity Interview Guide	
I declare that I will provide, in this Integrity Interview, information that is up-to-date, accurate, complete and honest, to the best of my knowledge and belief.	
I understand that there is a possibility that I may amend my answer(s) to any question(s) in the Integrity Interview by contacting the CBSA Personnel Security and Professional Standards Division.	
I understand that I do not have to provide any information in this Integrity Interview that relates to a conviction for which a pardon has been received, or a conviction that was processed pursuant to the <i>Young Offenders Act</i> or the <i>Youth Criminal Justice Act</i> .	
I understand that the information provided in this Integrity Interview may affect my possibilities for any other employment with, or at, the CBSA within the next two (2) years, and/or, where applicable, may affect my current employment with, or work at, the CBSA.	
I understand that if I admit to having committed one or a number of criminal offence(s), during the Integrity Interview, actions could be taken which could lead, ultimately, to the imposition of a sentence.	
I consent to my personal information being collected, used, and disclosed for the purposes identified on the foregoing Pages 2,3,4 and ,5 of the Integrity Interview Guide	
I consent to my personal information being used for security screening pursuant to the Treasury Board Policy on Government Security http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578 .	

Annex 34 - Integrity Interview Guide

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

"I, the undersigned, do consent to the disclosure of the preceding information including my photograph for its subsequent verification and/or use in an investigation for the purpose of providing a security screening assessment. By consenting to the above, I acknowledge that the verification and/or use in an investigation of the preceding information may also occur when the reliability status, security clearance or site access are updated or otherwise reviewed for cause under the Policy on Government Security.

My consent will remain valid until such time as any such reliability status, security clearance or site access clearance is no longer a requirement for my continued employment with the CBSA, or any successor thereto, my employment is terminated, I am deployed to a position with another employer within the Government of Canada, or I revoke my consent, in writing, to the Director General, Security and Professional Standards of the CBSA."

_____ Name of Applicant (print)	
_____	_____ Date

This Integrity Interview is not complete until you have read, understood, signed, and dated the **Final Declaration, Acknowledgment, and Consent**.

Final Declaration, Acknowledgment, and Consent of: _____
Name of Applicant (print)

I, the undersigned, hereby declare that the information I have provided in this Integrity Interview (referred to on this page as the preceding information) is up to date, accurate, complete, and honest, to the best of my knowledge and belief.

I further acknowledge that the verification and/or use of the preceding information may also occur when my reliability status, security clearance or site access - if issued - are updated or otherwise reviewed for cause under the Policy on Government Security.

If I provided statements containing criminal admissions, I acknowledge that the CBSA may use and/or disclose such information for a law enforcement or public safety purpose as described under the "Notice Regarding Misconduct, Criminal Offences and Risk to the Safety of Others" on Page 4 of this Integrity Interview Guide

Annex 34 - Integrity Interview Guide

CANADA BORDER SERVICES AGENCY

PROTECTED B

(Once completed)

Applicant Name: _____
(Print)

By my signature below, I declare that I have read and understand how the preceding information will be managed and I hereby consent to the use and disclosure of my personal information as described herein above.

Signature of Applicant

Date

Annex 36 - The Four-Part Test of R. v. Oakes for Necessity and Proportionality for the HIPSSS

Question 1: Is the measure demonstrably necessary to meet a specific need?

Justifications for the HIPSSS and all of its components were articulated in the May 2012 Treasury Board Submission for which policy approval was granted by Treasury Board Cabinet Ministers. As part of the annex to the PIA, we provided explanations and reasoning behind the 49 questions included in the Integrity Questionnaire. In addition, we adjusted the questions based on your feedback and have discontinued using the Questionnaire as a document that individuals complete and submit to the CBSA. You will note that we have changed question # 24 to reflect our discussions relating to potential blackmail or corruption. For your reference, further clarification is provided below.

CBSA employees work around the clock to keep goods and people moving across the Canadian border: collecting duties and taxes, supporting trade and ensuring that the border is secure and protected against potential threats to Canada's safety and security. The CBSA has a 100% service standard requirement, as border operations are required for maintaining the stability and prosperity of the Canadian economy.

This multi-faceted role has created the need for a higher degree of integrity among staff than for other departments and agencies and hence the need to deem all positions within the Agency as high integrity. Many aspects of the CBSA's work are vulnerable to corruption, fraud or infiltration by the criminal element, particularly since the CBSA has access to sensitive information and monopoly power over certain services, such as the release of cargo and conveyances and the clearance of passengers into Canada. If coerced by the criminal element, the CBSA's ability to provide effective integrated border services could be compromised. It could also impact public safety, public trust, relationships with domestic and international partners, and the economic well-being of the country and national security.

The CBSA has conducted internal investigations or received referrals relating to security concerns and serious misconduct in all areas of the organization, ranging from mail room clerks to executives. Given the nature of our mandate and the sensitive information and assets available to employees of the CBSA, even one case is too many and could cause grave injury to the country and its citizens. The CBSA has had to deal with cases involving major fraud, attempts at infiltration by organized crime, disclosure of classified information, facilitating the movement of contraband/drugs, and disclosing information to organized crime to name a few.

On an annual basis, the CBSA's Professional Standards Program reviews between 150 and 200 referrals of alleged employee misconduct and personnel security concerns. During the last three fiscal years, unauthorized disclosures of information and criminal association were amongst the top allegations reported to the program. In 2011-2012, there were 45 allegations of criminal association by CBSA employees. For the first half of this fiscal year, there have been 12 allegations of criminal association. Not all of these allegations have been proven; numerous remain outstanding or under investigation. Others are investigated by law enforcement and in some cases the Public Sector Integrity Commissioner.

Question 2: Is it likely to be effective in meeting that need?

Yes. To date, we have conducted approximately 350 interviews for external candidates to Border Services Officer (BSO) positions (150 between May and July 2013; and 200 between October 28 and November 30, 2013). Through our first set of interviews, we identified moderate to serious adverse security information for approximately one-third of the candidates. This ranged from criminal history and drug use, to the assault of a police officer and disturbing associations with members of organized crime. None of this information would have come to light under the CBSA's previous approach to personnel security screening.

Question 3: Is the loss of privacy proportional to the need?

Yes, the loss of privacy is proportional to the need. The CBSA recognizes the importance of collecting only enough information necessary for decision-making. As you are aware, while we are not asking applicants to submit written responses to the Integrity Questionnaire, we are using the document as a reference guide in conducting integrity interviews of new applicants to the CBSA to ensure everyone is being treated fairly in the interview process. This will add consistency in our procedures, and in conducting administrative investigations when we become aware of adverse information that puts an existing employee's Reliability Status screening into question. You will recall that for Reliability Status, we are concerned about employee or candidate Honesty, Integrity, and Trustworthiness. On an annual basis, we will conduct an internal review of the HIPSSS and will provide you a letter outlining the effectiveness of the tool to date, and all changes that we will introduce to ensure that we are collecting only enough information necessary for our decision-making.

Question 4: Is there a less privacy-invasive way of achieving the same end?

Unfortunately, there is not a less privacy-invasive way of achieving the same security screening results; however, we do ensure the confidentiality and safeguarding of the information collected for security screening purposes. We previously had a less rigorous security screening process based on the baseline requirements outlined in the TBS Personnel Security Standard.

Unfortunately, it did not result in the same level of thoroughness in our ability to detect threats and potential threats to the Agency as is evidenced by the suspensions and denials of Reliability Status since the implementation of the HIPSSS; particularly with the use of the Integrity Interview and corresponding Integrity Interview Guide.



Canada Border Services Agency High-Integrity Personnel Security Screening Standard (HIPSSS)

Enforcement Database Checks Integrity Interview Guide Psychological Testing

Privacy Impact Assessment (PIA)

Security and Professional Standards Directorate
Personnel Security and Professional Standards Division,
Comptrollership Branch
December 2013



Change Control Table

Version	Date	Change Made By	Change Requested By	Change
3	2012/02/20	Kory Beecroft	Lyne Pelletier	Updated PIA Template/Edits
4	2012/05/15	Margaret Cheliak	Sylvie Labrèche-Gravel	Updated PIA
5	2012/05/25	Kory Beecroft	Lyne Pelletier	Modifications/Edits
6	2012/05/29	Margaret Cheliak	Kory Beecroft	Modifications/Edits
7	2012/11/19	Catherine Power	Peter Pomerleau and Sylvie Labrèche-Gravel	Updated PIA Template/Edits
8	2013/01/08	K.McCarthy	Final OPI Review	Updated PIA Template / Edits
9	2013/09/10	K. McCarthy	OPC feedback – July 30, 2013	Updated PIA
10	2013/12/10	Catherine Power	Ken McCarthy	Modifications/Edits/New Annexes

PREAMBLE

The core Privacy Impact Assessment (core PIA) Template is a policy tool developed by the Treasury Board of Canada Secretariat (TBS) to assist government institutions in conducting core PIAs.

Table of Contents

PREAMBLE	2
EXECUTIVE SUMMARY	4
Treasury Board Secretariat (TBS) Policy on Government Security (PGS), Personnel Security Standard	4
DEFINITIONS	6
SECTION 1 - OVERVIEW AND INITIATION	7
Treasury Board Secretariat (TBS) Policy on Government Security (PGS), Personnel Security Standard	11
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	13
1. Type of Program or Activity	13
2. Type of Personal Information Involved and Context	14
3. Program or Activity Partners and Private Sector Involvement	14
4. Duration of the Program or Activity	15
5. Program Population	15
6. Technology and Privacy	16
7. Personal Information Transmission	17
8. Risk Impact to the Institution	17
9. Risk Impact to the Individual or Employee	18
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	19
SECTION 4 - FLOW OF PERSONAL INFORMATION	23
4.1 Example of a Data Flow Model – Diagram - **SEE ANNEX 6 FOR DETAILED DATA FLOW**	23
4.2 Example of a Data Flow Model - Table	23
4.3 Internal Use and Disclosure	24
4.4 External Use and Disclosure	25
4.5 Retention / Storage	25
4.6 Other Possible Considerations	26
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	27
1. Legal Authority for Collection of Personal Information	27
2. Necessity to Collect Personal Information	28
3. Authority for the Collection, Use or Disclosure of the Social Insurance Number ..	28
4. Direct Collection - Notification and Consent (as appropriate)	29
5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations ..	30
6. Indirect Collection - Without Notification and Consent	31
7. Retention and Disposal of Personal Information	32
8. Accuracy Of Personal Information	32
9. Use Of Personal Information	34
10. Disclosures Directly Related to the Administration of the Program or Activity	35
11. Accounting For New Uses or Disclosures Not Reported in Info Source	37
12. Safeguards - Statement Of Sensitivity	38
13. Safeguards - Threat and Risk Assessment	39
14. Safeguards - Administrative, Physical and Technical	40
15. Technology and Privacy - Tracking Technologies	42

16. Technology and Privacy - Surveillance or Monitoring	42
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement ..	43
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS.....	46
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	54
SECTION 8 - FORMAL APPROVAL.....	55

EXECUTIVE SUMMARY

In November 2007, the Canada Border Services Agency (CBSA) Executive Management Committee approved the development of all required processes to implement enhanced personnel security screening measures through the creation of the CBSA High-Integrity Personnel Security Screening Standard (HIPSSS). These measures were designed to decrease the risk of infiltration and corruption and maintain program integrity as required under the Policy on Government Security (PGS) for all CBSA positions. The CBSA put forward a Treasury Board (TB) Submission to obtain the required Policy approval from the TB Cabinet Ministers Committee. Approval to proceed with the HIPSSS implementation was obtained at the May 31, 2012 Committee meeting. Three versions of this Privacy Impact Assessment have been filed with the Office of the Privacy Commissioner (OPC): the first in May 2012; and updated versions in November 2012 and February 2013 in response to OPC feedback. This is the fourth and final version of the HIPSSS Privacy Impact Assessment. The following information applies to the HIPSSS:

Treasury Board Secretariat (TBS) Policy on Government Security (PGS), Personnel Security Standard

The TBS PGS, Personnel Security Standard¹ outlines the baseline Personnel Security Screening Process for the Government of Canada. The process sees the collection of personal information for an individual (potential or current employee or other individuals working at the CBSA) by way of a criminal record check, credit check, fingerprint check, a Residency and Travel Outside Canada Questionnaire (Previously submitted annex 27_RTOC.), CSIS indices checks (when applicable), employment/education verifications and when required, a subject interview. This information is collected with the informed consent of the individual prior to conducting any of the checks above mentioned. This information is protected in accordance with the Financial Administration Act and the Policy on Government Security.

New High Integrity Personnel Security Screening Process

The change to the former personnel security screening process involved the implementation of enhanced security screening initiatives for potential new employees to or individuals coming to work at the CBSA and existing staff when a determination to grant, deny or revoke a security screening (Reliability Status) is made prior to processing a security clearance (i.e., Secret and Top Secret).

The additional integrity tools and background checks under the HIPSSS include: Royal Canadian Mounted Police (RCMP) Law Enforcement Checks; CBSA enforcement database checks; an Integrity interview, open source checks (for cause only) and a Psychological Ethical Judgement Test administered (for cause only). When the CBSA first implemented the HIPSSS in June 2012, it had intended to use a written Integrity Questionnaire for all candidates. In the months that followed and with feedback from

¹ <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12330§ion=text>

the OPC, the CBSA discontinued the use of the written questionnaire in October 2012. The written Questionnaire has been replaced with Integrity Interviews and the questions from the Questionnaire were modified based on consultation with the OPC and other stakeholders and used to develop an Integrity Interview Guide, henceforth referred to as the Guide. The Guide was implemented in May 2013. The Guide is used during face-to-face Integrity Interviews as part of the Reliability Status screening for Border Services Officer recruitment and for the recruitment of other individuals coming to work at the CBSA. Law Enforcement Record Checks and CBSA enforcement database checks will apply to existing employees upon security screening renewal and when an upgrade to their security screening is required to support a new position. The Integrity Interview may also apply to existing employees for cause if adverse information² is found. Please note that these types of Integrity or subject interviews have been authorized under the Treasury Board of Canada Secretariat's Policy on Government Security, Personnel Security Standard since 2002.

Additional verifications may be administered to assess an individual's integrity at time of application, when adverse information has been uncovered concerning an individual or when a review for cause investigation is launched based on adverse information that may affect an existing employee's security screening level. The implementation of these additional verifications for existing employees and new applicants to the CBSA occurred after Treasury Board approval and consultation with the Unions representing the Agency's employees had taken place. The collection, retention and disclosure of information from the above noted checks abide by the Financial Administration Act, the TBS Policy on Government Security, and the TBS Personnel Security Standard.

Personnel Security Screening decisions based on the personal information collected through the HIPSSS may be shared internally within the CBSA, with staffing, Labour Relations, Legal Services and Hiring Managers when Reliability Status is denied or revoked. However, the personal information itself will not be shared. Relevant information (ethics and integrity concerns) may also be shared with a psychologist when psychological testing for cause is required.

The personal information is safeguarded electronically on the CBSA Personnel Security Screening Database (Protected B), Case Management System (Secret) and physically in the Personnel Security Screening Section's file room which has been security cleared to Secret. CBSA has strong safeguards in place for both the physical and digital storage of personal information related to the HIPSSS. The safeguarding procedures have been consolidated in the previously submitted Annex 3 - Annex E of the HIPSSS Standard Operating Procedures.

Anyone requiring a CBSA security screening will be screened through the HIPSSS. This includes all CBSA employees (permanent, term, casual, and part-time), contract and private agency personnel, and individuals seconded or assigned to CBSA (including students). Security screening requirements are identified as a condition of employment or an agreement (i.e. written collaborative arrangement or agreement).

- In addition to the baseline verifications of employment history, credit and criminal record checks that are currently being conducted, individuals who are not employees and

² Adverse Information is information that can reasonably be cause to believe that the individual may steal valuables, exploit assets and information for personal gain, fail to safeguard information and assets entrusted to him or her, or exhibit behaviour that would reflect negatively on their reliability. <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12330§ion=text>

individuals who are being considered for employment with the CBSA will also undergo the following verifications:

- Law Enforcement Record Checks
 - Internal data base checks
 - Integrity interviews
 - Other checks may be undertaken for cause on a case by case basis.
- All individuals, upon renewal or upgrade to their CBSA security screenings will undergo the following verifications:
 - Law Enforcement Record Checks
 - Internal data base checks
 - Integrity interviews (for cause)
 - Other checks may be undertaken for cause on a case by case basis.
 - In addition, all armed officers who do not hold a valid Possession and Acquisition Licence (PAL) or who have not yet been screened through the HIPSSS, will be screened through the HIPSSS in advance of their normal renewal cycle.

ABBREVIATIONS AND ACRONYMS

Note: Using the format below, list any abbreviations and acronyms that are used in this report.

The following is a list of abbreviations and acronyms used in this report:

ATIP	Access to Information and Privacy
CBSA	Canada Border Services Agency
HIPSSS	High-Integrity Personnel Security Screening Standard
MOU	Memorandum of Understanding
LOI	Letter of Intent
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PGS	Policy on Government Security
COR	Class of Record
TBS	Treasury Board Secretariat
CIC	Citizenship & Immigration Canada
RCMP	Royal Canadian Mounted Police
CSIS	Canadian Security Intelligence Service
ICES	Integrated Customs Enforcement System

DEFINITIONS

Note: Using the format below, provide definitions of the terms frequently used in this report.

Name of Program / Activity / Service	PIA
--------------------------------------	-----

This section provides definitions of the terms frequently used in this report:

Administrative purpose	The <i>Privacy Act</i> defines an “administrative purpose” to be the use of an individual’s personal information in a decision-making process that directly affects that individual.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled? This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Info Source	Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person? The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.

SECTION 1 - OVERVIEW AND INITIATION

Government Institution: **Canada Border Services Agency (CBSA)**

Government Official Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the <i>Privacy Act</i>
Claude Rochette Vice President Comptrollership Branch, CBSA	Dan Proulx Director - ATIP, CBSA

Name of Program or Activity of the Government Institution: **High-Integrity Personnel Security Screening Standard**

Description of Program or Activity: **Management and Oversight Services**

Management and Oversight Services involve activities undertaken for determining strategic direction, and allocating resources among services and processes, as well as those activities related to analyzing exposure to risk and determining appropriate countermeasures. They ensure that the service operations and programs of the federal government comply with applicable laws, regulations, policies, and/or plans. Service Groupings for Management and Oversight Services include: Strategic Policy and Planning and Government Relations (incl. Federal / Provincial / Territorial / International); Executive Services; Corporate Policy, Standards, Guidelines; Program / Service Management; Investment Planning; Project Management; Risk Management; Performance and Reporting; Internal Audit; Evaluation.

Note: This should align with the program named and described in the institution’s Info Source Chapter as required under section 5 of the *Access to Information Act*. For institutions that develop a Program Activity Architecture (PAA) as per the Management, Resources, and Results Structure Policy, the institutional Info Source chapter must align with the programs, activities and sub-activities described in the PAA.

Description of the class of records associated with the program or activity:

Name of Program / Activity / Service	PIA
<p>Description: Includes records related to personnel security screening, recruitment and staffing of individuals to fill all positions including contracts within the Canada Border Services Agency (CBSA). Records will have information related to security screening, which may include examining, testing, interviewing, assessing, selecting, hiring and promoting candidates for employment. May also include information related to terms and conditions of employment (including conflict of interest), deployments, assignments, secondments, student, professional, and occupational recruitment, post-employment appeals, and area of selection, as well as information received from or shared with central agencies responsible for security screening, recruitment and staffing, other employment agencies, or both.</p>	
<p>Note: Relevant information may be transferred to an employee's personnel file if the individual accepts an offer of employment from the institution.</p>	
<p>Document Types: Unsolicited résumés, interview questions and answers, security screening forms, Integrity Questionnaire received and used in the screening process prior to October 25, 2012^[1], CBSA Residency and Travel Outside of Canada form, competition related information, reference check information, candidate and security screening inquiries and responses, copies of letters of offer, ratings board assessments, information within automated or Web-based application tools, second language evaluation results, identification, professional qualification and education documentation, credit check information, fingerprints including related database information, all documentation, reports/tapes/notes from Integrity Interviews and psychological test results (pass or fail).</p>	
<p>Record Number: CBSA CMT 1120</p>	

Class of Record Number: **CBSA CMT 1120**

☒ Proposal for a New Personal Information Bank

[1] In cases where the Questionnaire was submitted prior to October 25th and was already used as part of the screening process, the Policy on Government Security obligates the CBSA to retain the information for a minimum of two years and to safeguard it at the Protected B level.

Personnel Security Screening Program

Description: This bank describes information about current and prospective employees who must undergo a security screening assessment to gain or maintain employment with the Canada Border Services Agency. The data in the bank describes personal information about the subject and his or her immediate family which may include criminal associations and/or other factors that may be relevant to the file. It may also include results of name or fingerprint criminal record checks, pending charges, encounters with law enforcement, driver's abstract, credit bureau checks, Canadian Security Intelligence Service (CSIS) indices checks, open source Internet checks, Integrity Questionnaire received and used in the screening process prior to October 25, 2012, reports/tapes/notes from Integrity Interviews, psychological test results (pass or fail), related correspondence, administrative investigative reports related to interviews and findings, outcome and related information / documents with neighbours, previous employers, character references and an analysis of the information. Personal information may include biographical information, biometric information (fingerprints), citizenship status, contact information, credit information, date of birth, educational information, employee identification number, employee personnel information, financial information, name, signature, other (driver's licence number). In addition, it includes the level of security clearance issued or reliability status granted and the reasons the latter was denied or revoked, as the case may be.

Note: Individuals requesting information described by this bank must provide the competition number and/or Personal Record Identifier.

Class of Individuals: All current employees, individuals applying to become an employee of the Canada Border Services Agency (CBSA), former employees, agency, casual, seasonal, student and term employees, contractors/consultants, full or part time employees of the Canada Border Services Agency (CBSA), immediate relatives, current and former spouse / common law partner, and individuals who give character references..

Purpose: Personal information is used to support decisions for granting, denying, revoking or reviewing for cause the reliability status, security clearance or site access of individuals working or applying to work through appointment, assignment or contract. A review for cause investigation may result in the revocation of the individual's reliability status, security clearance or site access. Personal information is collected pursuant to subsection 7(1), 11.1(1) and 12(1) (e) of the Financial Administration Act (FAA) and as required under the Policy on Government Security and in accordance with the Canada Border Services Agency (CBSA) Departmental Security Policy, Sections 5 and 11 of the Canada Border Services Agency Act and Section 31 of the Public Service Employment Act.

Consistent Uses: The information may be used or disclosed for the following purpose: conducting reliability personnel security screening checks, conducting database checks, audit, statistical, periodic data matching and to assess an individual's loyalty and reliability as it relates to loyalty. Information may be shared with the Canadian Security Intelligence Service (CSIS), Security Assessments/Advice (SIS PPU 005), the Royal Canadian Mounted Police (RCMP), Forensic Science and Identification Services and Canadian Criminal Real Time Identification Services (CMP PPU 030 005), as service providers in accordance with the Policy on Government Security and the Royal Canadian Mounted Police (RCMP), Operational Case Records (CMP PPU 005) for database checks. The status may be shared with CBSA internal Human Resources officials, refer to Standard Personal Information Bank Employee Personnel Record (PSE 901). Information may be shared with entities outside the federal government, including credit bureaus.

PIA: A Privacy Impact Assessment (PIA) was completed in May 2012, and updated in November 2012, January 2013 and December 2013.

Name of Program / Activity / Service

PIA

Related Class of Record Number: CBSA CMT 1120

TBS Registration: TBD

Bank Number: CBSA PPU 1108

Retention and Disposal Standards: Records will be retained for 2 years after an employee has left Canada Border Services Agency (CBSA) and then records are destroyed. If a security level is revoked or denied, records will be retained for 5 years and then destroyed.

RDA Number: 98-005

Legal Authority for Program or Activity:

Section 7, 11.1(1) and 12(1) (e) of the Financial Administration Act, Sections 5 and 11 of the Canada Border Services Agency Act and Section 31 of the Public Service Employment Act.

Note: Prior to proceeding with the assessment it is essential that Parliamentary authority for the relevant program or activity be established. Generally, Parliamentary authority is usually contained in an Act of Parliament or subsequent regulations, or approval of expenditures proposed in the Estimates and authorized by an *Appropriations Act*. If legal authority is unclear consult your Legal Service to determine authority for the program or activity. (See question 1 of **Section 5**)

Summary of the project / initiative / change:

Name of Program / Activity / Service	PIA
--------------------------------------	-----

Note: Short description of the institutions business objectives, project objectives, project / initiative / change scope, product scope, stakeholders and assumptions. This PIA reflects the program as of September 2013.

In November 2007, the Canada Border Services Agency (CBSA) Executive Management Committee approved the development of all required processes to implement enhanced personnel security screening measures allowable to decrease the risk of infiltration and corruption and maintain program integrity under the Policy on Government Security for all CBSA positions; and the creation of a CBSA High-Integrity Personnel Security Screening Standard (HIPSSS). The following information applies to the HIPSSS:

Treasury Board Secretariat (TBS) Policy on Government Security (PGS), Personnel Security Standard

The TBS PGS, Personnel Security Standard³ outlines the baseline Personnel Security Screening Process for the Government of Canada. The process sees the collection of personal information for an individual (potential or current employee) by way of a criminal record check, credit check, fingerprint check, a Residency and Travel Outside Canada Questionnaire (Previously submitted annex 27_RTOC.), CSIS indices checks (when applicable) employment/education verifications and when required, a subject interview. This information is collected with the informed consent of the individual prior to conducting any of the checks above mentioned. This information is protected in accordance with the Financial Administration Act and the Policy on Government Security.

New High Integrity Personnel Security Screening Process

The change to the current personnel security screening process involves the implementation of enhanced security screening initiatives for potential new employees to the CBSA and existing staff when a determination to grant, deny or revoke a security screening (Reliability Status) is made prior to processing a security clearance (i.e., Secret and Top Secret).

The additional integrity tools and background checks under the HIPSSS include:

Royal Canadian Mounted Police (RCMP) Law Enforcement Checks; CBSA enforcement database checks; an Integrity interview and a Psychological Ethical Judgement Test administered for cause only. When the CBSA first implemented the HIPSSS in June 2012, it had intended to use a written Integrity Questionnaire for all candidates. In the months that followed and with feedback from the OPC, the CBSA discontinued the use of the written questionnaire in October 2012. The written Questionnaire has been replaced with Integrity Interviews and the questions from the Questionnaire were modified based on consultation with the OPC and other stakeholders and used to develop an Integrity Interview Guide, henceforth referred to as the Guide. The Guide was implemented in May 2013. It is used in the face-to-face Integrity Interviews as part of the Reliability Status screening for Border Services Officer recruitment and for the recruitment of other individuals coming to work at the CBSA. Enforcement database checks will apply to existing employees upon security screening renewal and when an upgrade to their security screening is required to support a new position. Depending on the circumstances of the case, the Integrity Interview may also apply to existing employees. Please note that these types of interviews have been authorized under the Treasury Board of Canada Secretariat's Policy on Government Security, Personnel Security Standard since 2002.

³ <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12330§ion=text>

Additional verifications may be administered to assess an individual's integrity at time of application, when adverse information has been uncovered concerning an individual or when a review for cause investigation is launched based on adverse information that may affect an existing employee's security screening level. The implementation of these additional verifications for existing employees and new applicants to the CBSA occurred after Treasury Board approval and consultation with the Unions representing the Agency's employees had taken place. The collection, retention and disclosure of information from the above noted checks abide by the Financial Administration Act, the TBS Policy on Government Security, and the TBS Personnel Security Standard.

The personal information is safeguarded electronically on the CBSA Personnel Security Screening Database (Protected B), Case Management System (Secret) and physically in the Personnel Security Screening Section's file room which has been security cleared to Secret. CBSA has strong safeguards in place for both the physical and digital storage of personal information related to HIPSSS. The safeguarding procedures have been consolidated in the previously submitted Annex 3 - Annex E of the HIPSSS Standard Operating Procedures.

Personnel Security Screening decisions based on the personal information collected through the HIPSSS may be shared internally within the CBSA, with staffing, Labour Relations, Legal Services and Hiring Managers when Reliability Status is denied or revoked. However, the personal information itself will not be shared. Relevant information (ethics and integrity concerns) may also be shared with a psychologist when psychological testing for cause is required.

Anyone requiring a CBSA security screening will be screened through the HIPSSS. This includes all CBSA employees (permanent, term, casual, and part-time), contract and private agency personnel, and individuals seconded or assigned to CBSA (including students). Security screening requirements are identified as a condition of employment or an agreement (i.e. written collaborative arrangement or agreement).

- In addition to the baseline verifications of employment history, credit and criminal record checks that are currently being conducted, individuals who are not employees and individuals who are being considered for employment with the CBSA will also undergo the following verifications:
 - Law Enforcement Record Checks
 - Internal data base checks
 - Integrity interviews
 - Other checks may be undertaken for cause on a case by case basis.
- All individuals, upon renewal or upgrade to their CBSA security screenings will undergo the following verifications:
 - Law Enforcement Record Checks
 - Internal data base checks
 - Integrity interviews (for cause)
 - Other checks may be undertaken for cause on a case by case basis.

Name of Program / Activity / Service

PIA

- In addition, all armed officers who do not hold a valid Possession and Acquisition Licence (PAL) or who have not yet been screened through the HIPSSS, will be screened through the HIPSSS in advance of their normal renewal cycle.

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

For Section 2, please check the appropriate box that describes the level of risk related to your program or activity and provide details.

1. Type of Program or Activity	Level of Risk
Program or activity that does NOT involve a decision about an identifiable individual Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual. The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information.	<input type="checkbox"/> 1
Administration of Programs / Activity and Services Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).	<input checked="" type="checkbox"/> 2
Compliance / Regulatory investigations and enforcement Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e., a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).	<input type="checkbox"/> 3
Criminal investigation and enforcement / National Security Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).	<input type="checkbox"/> 4
Details: CBSA employees work around the clock to keep goods and people moving across the Canadian border: collecting duties and taxes, supporting trade and ensuring that the border is secure and protected against potential threats to Canada's safety and security. The CBSA has a 100% service standard requirement, as border operations are required for maintaining the stability and prosperity of the Canadian economy. Specific CBSA responsibilities include: <ul style="list-style-type: none"> • administering legislation (over 90 acts) that governs the admissibility of people, goods and plants and animals into and out of Canada; • detaining those people who may pose a threat to Canada; • identifying and removing people who are inadmissible to Canada, including those involved in terrorism, organized crime, war crimes or crimes against humanity; • interdicting illegal and strategically sensitive goods entering or leaving the country; • protecting food safety, plant and animal health, and Canada's resource base; • promoting Canadian business and economic benefits by administering trade legislation and trade agreements to meet Canada's international obligations, including the enforcement of trade remedies that help protect Canadian industry from the injurious effects of dumped and subsidized imported 	

Name of Program / Activity / Service	PIA
--------------------------------------	-----

goods; and

- collecting applicable duties and taxes on importing goods.

This multi-faceted role has created the need for a higher degree of integrity among staff than for other departments and agencies and hence the need to deem all positions within the Agency as high integrity. Many aspects of the CBSA's work are vulnerable to corruption, fraud or infiltration by the criminal element, particularly since the CBSA has access to sensitive information and monopoly power over certain services, such as the release of cargo and conveyances and the clearance of passengers into Canada. If coerced by the criminal element, the CBSA's ability to provide effective integrated border services could be compromised. It could also impact public safety, public trust, relationships with domestic and international partners, and the economic well-being of the country and national security.

As an integral part of public safety, and in accordance with the Canada Border Services Agency (CBSA) mandate, the Agency is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants that meet all requirements under the program legislation. As a result, every day CBSA employees make thousands of real-time decisions that directly affect the security and prosperity of Canada.

2. Type of Personal Information Involved and Context	Level of Risk
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	<input type="checkbox"/> 1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	<input type="checkbox"/> 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	<input type="checkbox"/> 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	<input checked="" type="checkbox"/> 4
Details: In order to fulfill our mandate of ensuring the security and prosperity of Canada by managing access of people and goods to and from Canada, we must ensure that all employees of the CBSA conduct themselves with integrity, respect and professionalism. In order to do this we must collect and analyze sensitive personal information via our Personnel Security Screening Process.	

3. Program or Activity Partners and Private Sector Involvement	Level of Risk
Within the institution (amongst one or more programs within the same institution)	<input type="checkbox"/> 1
With other federal institutions	<input checked="" type="checkbox"/> 2
With other or a combination of federal/ provincial and/or municipal government(s)	<input type="checkbox"/> 3
Private sector organizations or international organizations or foreign governments	<input checked="" type="checkbox"/> 4
Details: Tombstone data is provided to the following organizations:	
<ul style="list-style-type: none"> • A contracted Private Sector psychologist for the purposes of psychological testing. Responses are evaluated by the psychologist and Pass/Fail response is provided to the CBSA to support security 	

Name of Program / Activity / Service	PIA
<p>screening. (previously submitted Annex 8)</p> <ul style="list-style-type: none"> • Equifax Canada, a Private Sector credit bureau for the purpose of collecting credit information to support security screening (as per the PGS and used by Government of Canada departments and agencies). Equifax provides the CBSA with a complete credit report which is then used in screening analysis. (previously submitted Annex 12) <p>Information is collected by Royal Canadian Mounted Police (RCMP) – Screening/Reliability Screening Records CMP PPU 065, the Canadian Security Intelligence Service (CSIS) – Employee Security SIS PPE 815 for the purpose of personnel security screening (previously submitted Annex 28)</p>	

4. Duration of the Program or Activity	Level of risk
<p>One time program or activity</p> <p>Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.</p>	<input type="checkbox"/> 1
<p>Short-term program</p> <p>A program or an activity that supports a short-term goal with an established "sunset" date.</p>	<input type="checkbox"/> 2
<p>Long-term program</p> <p>Existing program that has been modified or is established with no clear "sunset".</p>	<input checked="" type="checkbox"/> 3

Details: As an integral part of public safety, and in accordance with the Canada Border Services Agency (CBSA) mandate, the agency is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants that meet all requirements under the program legislation. As a result, every day CBSA employees make thousands of real-time decisions that directly affect the security and prosperity of Canada. Many aspects of the CBSA's work are vulnerable to corruption or infiltration by the criminal element, particularly since the CBSA has monopoly power over certain services, such as the release of cargo and conveyances and the entry of people into Canada.

5. Program Population	Level of Risk
The program affects certain employees for internal administrative purposes.	<input type="checkbox"/> 1
The program affects all employees for internal administrative purposes.	<input checked="" type="checkbox"/> 2
The program affects certain individuals for external administrative purposes.	<input checked="" type="checkbox"/> 3
The program affects all individuals for external administrative purposes.	<input type="checkbox"/> 4

Details: As an integral part of public safety, and in accordance with the Canada Border Services Agency (CBSA) mandate, the agency is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants that meet all requirements under the program legislation. As a result, every day CBSA employees make thousands of real-time decisions that directly affect the security and prosperity of Canada. Many aspects of the CBSA's work are vulnerable to corruption or infiltration by the criminal element, particularly since the CBSA has monopoly power over certain services, such as the release of cargo and conveyances and the entry of people into Canada. Other individuals not employed by but working at the CBSA are also screened through the HIPSSS, such as contractors, private agency personnel and others who come to work on CBSA premises. These individuals may have access to the CBSA's sensitive information and assets and thus, must be screened to the same standard as CBSA employees.

Name of Program / Activity / Service	PIA
6. Technology and Privacy	
6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
6.2. Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Please specify:	
<p>The CBSA uses the Professional Standards Case Management System (PSCMS) to store all HIPSSS information (previously submitted Annex 9). PSCMS, which was originally purchased for the Professional Standards Investigations Section, has been customized for HIPSSS to create a segregated area of the system which can only be accessed on a need to know basis for personnel security screening purposes. It has full tracking capabilities for global assessment and review for cause information.</p>	
6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:	
6.3.1 Enhanced identification methods:	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
<p>This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).</p>	
Please specify:	
<p>Conducting mandatory digital fingerprint verifications as part of the security screening process is supported by the <i>Policy on Government Security</i> (PGS) and the <i>Treasury Board Secretariat</i> (TBS). Due to the mandate and sensitive nature of its information and assets, the CBSA moved forward with the implementation of mandatory digital fingerprints. This was implemented prior to the implementation of the HIPSSS in 2011 for all new Border Services Officer recruits to minimize potential security risks and preserve program integrity.</p>	
6.3.2 Use of Surveillance:	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<p>This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.</p>	
6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
<p>For the purposes of the Directive on PIA, government institutions are to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to</p>	

Name of Program / Activity / Service	PIA
--------------------------------------	-----

predict behaviour.

Please specify:

Data matching activities take place with our HIPSS partners – RCMP, CSIS (previously submitted Annex 28) – in order to validate and substantiate information provided by individuals being subjected to the CBSA Personnel Security Screening process.

A YES response to any of the above indicates the potential for privacy concerns and risks that will need to be considered and if necessary mitigated.

7. Personal Information Transmission	Level of Risk
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	<input type="checkbox"/> 1
The personal information is used in system that has connections to at least one other system.	<input checked="" type="checkbox"/> 2
The personal information is transferred to a portable device or is printed. USB key, diskette, laptop computer, any transfer of the personal information to a different medium.	<input type="checkbox"/> 3
The personal information is transmitted using wireless technologies.	<input type="checkbox"/> 4

Details: A Database called "Agency Personnel Screening System" (APSS) was carried over from Canada Revenue Agency (CRA) when the CBSA was created. It is used to collect and process Protected B information to support the Personnel Security Screening program for the CBSA. This ACCESS program houses screening records (approx. 16,000) for all employees and contractors in the Agency, which must be protected in accordance with legislation and other privacy policies against unauthorized destruction or disclosure. It has connectivity that allows it to transmit personal information to the RCMP and CSIS for personnel security screening processes. Digital fingerprints are also transmitted electronically from an external service provider to the RCMP, which will be sent directly to the RCMP in the near future. A Personnel Security Screening Statement of Sensitivity (previously submitted Annex 2) was conducted on the APSS system and all recommendations were applied.

The APSS does not contain all of the protected client information. It contains tombstone information (name, date of birth, address, etc.) that is transmitted to the RCMP to enable them to conduct criminal record name checks and the Law Enforcement Record Checks (LERCS); and to the credit bureau to allow for a credit check to be conducted. Information such as Integrity interviews and all other information contained in the individual's security screening application forms are retained in a paper file located in a file area that satisfies the Government of Canada Secret requirements. Access to those files is limited to security screened staff that have a right and need to know the information. To eliminate unlawful disclosures, a disclosure form and procedures were implemented to ensure need to know is strictly enforced. Future enhancements to systems such as APSS will include audit trail capabilities.

While the CBSA uses the Professional Standards Case Management System (PSCMS) originally known as the IA Pro (previously submitted Annex 9) to store all HIPSS information, it is a stand-alone system with no connectivity to any other systems or networks. Although considered low risk due to its lack of connectivity, a TRA and a Statement of Sensitivity will be conducted.

8. Risk Impact to the Institution	Level of Risk
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	<input type="checkbox"/> 1

Name of Program / Activity / Service	PIA
Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	<input type="checkbox"/> 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	<input type="checkbox"/> 3
Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	<input checked="" type="checkbox"/> 4

Details: Should the agency not implement the enhanced security screening initiatives, the risk posed to the agency's reputation will be high. There is currently an increase in employee corruption, some of which has been highly publicized in the media causing embarrassment to the agency and a loss of credibility. Should this corruption not be mitigated, the impacts to the Agency are as follows:

- * Potential infiltration of organized crime.
- * Loss of law enforcement partners' confidence and trust in the Agency.
- * Loss of confidence in the Security and Professional Standards Program by Agency employees.
- * Erosion of public trust including scrutiny of elected officials.
- * Increased risk of unauthorized access, loss, theft, tampering, disclosure and compromise of sensitive assets and information.
- * Inability to meet its mandate set forth by the Government of Canada.
- * Inability to achieve its strategic outcomes as identified in the RPP.

9. Risk Impact to the Individual or Employee	Level of Risk
Inconvenience.	<input type="checkbox"/> 1
Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
Financial harm.	<input type="checkbox"/> 3
Physical harm.	<input type="checkbox"/> 4

Details: The type of information that will be gathered deals with an individual's criminal history, customs or immigration violations, immigration history, driving history, alcohol/drug use, gambling, security issues, use of force, unlawful sexual activity, involvement with law enforcement, employment, involvement with computers or technology, lifestyle and your psychological state. This information, if divulged, could have a negative effect on the individual's reputation and could cause embarrassment.

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

Note: Identification of sub-elements is necessary where sensitive personal information is being collected or where the type of program or activity presents a potential privacy risk at level 2-3-4 in "Section 2 - Risk Identification and Categorization" of the core PIA.

****Please consult previously submitted Annex 5, Annex 6 and Annex 7 for more detailed Personal Information Elements and Sub-elements****

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
**Annex 5_Integrity Questionnaire				Annex 6_IQ Justification Preamble Annex 7_IQ Justification chart
Personnel Management	Personal Identifiers	Employee ID / PRI / Rank & Service Number	Paper Forms: <u>TBS 330-23</u> (Annex 14)	To identify clients
Biographical Information	Name	First Name / Middle Initial / Last Name / Family Name at Birth/ All Other Names Used (nicknames) / Name Change (other than marriage)	Paper Forms: <u>TBS 330-23</u> Integrity Questionnaire	To identify clients.
Biographical Information	Gender	Male / Female	Paper Forms: <u>TBS 330-23</u> <u>TBS 330-60</u> (Annex 15)	To identify clients.
Biographical Information	Date of Birth	YYYY / MM / DD	Paper Forms: <u>TBS 330-23</u> <u>TBS 330-60</u>	To identify clients.
Biographical Information	Place of Birth	City / Province/State / Country	Paper Forms: <u>TBS 330-23</u>	To identify clients.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
			<u>TBS 330-60</u>	
Biographical Information	Contact Information	Telephone number(s) / Email Address / Home Address(es) (10 yrs) / Dates Lived At Address(es)	Paper Forms: <u>TBS 330-23</u> <u>TBS 330-60</u> Integrity	To identify clients.
Biographical Information	Citizenship	Present Citizenship and Dual Citizenship / Naturalized Canadian Certificate Number / Immigrant Visa-Record of Landing	Paper Form: <u>TBS 330-60</u>	To identify clients.
Family	Marital Status	Married / Common-Law Partnership / Separated / Widowed / Divorced / Single	Paper Form: <u>TBS 330-60</u>	To identify clients and partners/associates.
Family	Current Spouse/Common-Law Partner Information	Current Spouse/Common-Law Partner First & Last Name / Maiden Name / Current Spouse/Common-Law Partner Present Citizenship / Date of Marriage/ Common-Law Partnership/ Date of Marriage/ City, Province or State & Country of Marriage/Common-Law Partnership / Birth City, Province or State & Country of Spouse/ Common-Law Partner / Date of Birth of Spouse/ Common-Law Partner / Present Address of Spouse/ Common-Law Partner / Date of Separation, Divorce or Widowing / Job Title, Name & Address of Spouse/ Common-Law Partners' Employer	Paper Form: <u>TBS 330-60</u>	To assess reliability status/loyalty.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
Family	Previous (cover only past 5 yrs) Spouse/Common-Law Partner Information	Previous Spouse/Common-Law Partner First & Last Name / Previous Spouse/Common-Law Partner Present Citizenship / Date of Previous Marriage / City, Province or State & Country of Previous Marriage/Common-Law Partnership / Date of Separation, Divorce or Widowing of Previous Marriage/Common-Law Partnership / City, Province or State & Country of Separation, Divorce or Widowing of Previous Marriage/Common-Law Partnership / Country of Birth of Previous Marriage/Common-Law Partner / Date of Birth of Previous Marriage/Common-Law Partner	Paper Form: <u>TBS 330-60</u>	To assess reliability status/loyalty.
Family	Immediate Relatives Note: Immediate Family includes: All children 18+ yrs of age and older that you or your spouse/common-law partner have a parental relationship; Your Father, Mother, Brothers, Sisters – including "half" or "step" relatives; Your current spouse's or common-law partner's father and mother – including "half" or "step" relatives;	Full Name / Relationship / City, Province, Territory or State & Country of Birth / Date of Birth / Present Address / Date of Death (if applicable) / Name & Address of Employer / Job Title	Paper Form: <u>TBS 330-60</u>	To assess reliability status/loyalty.

Name of Program / Activity / Service

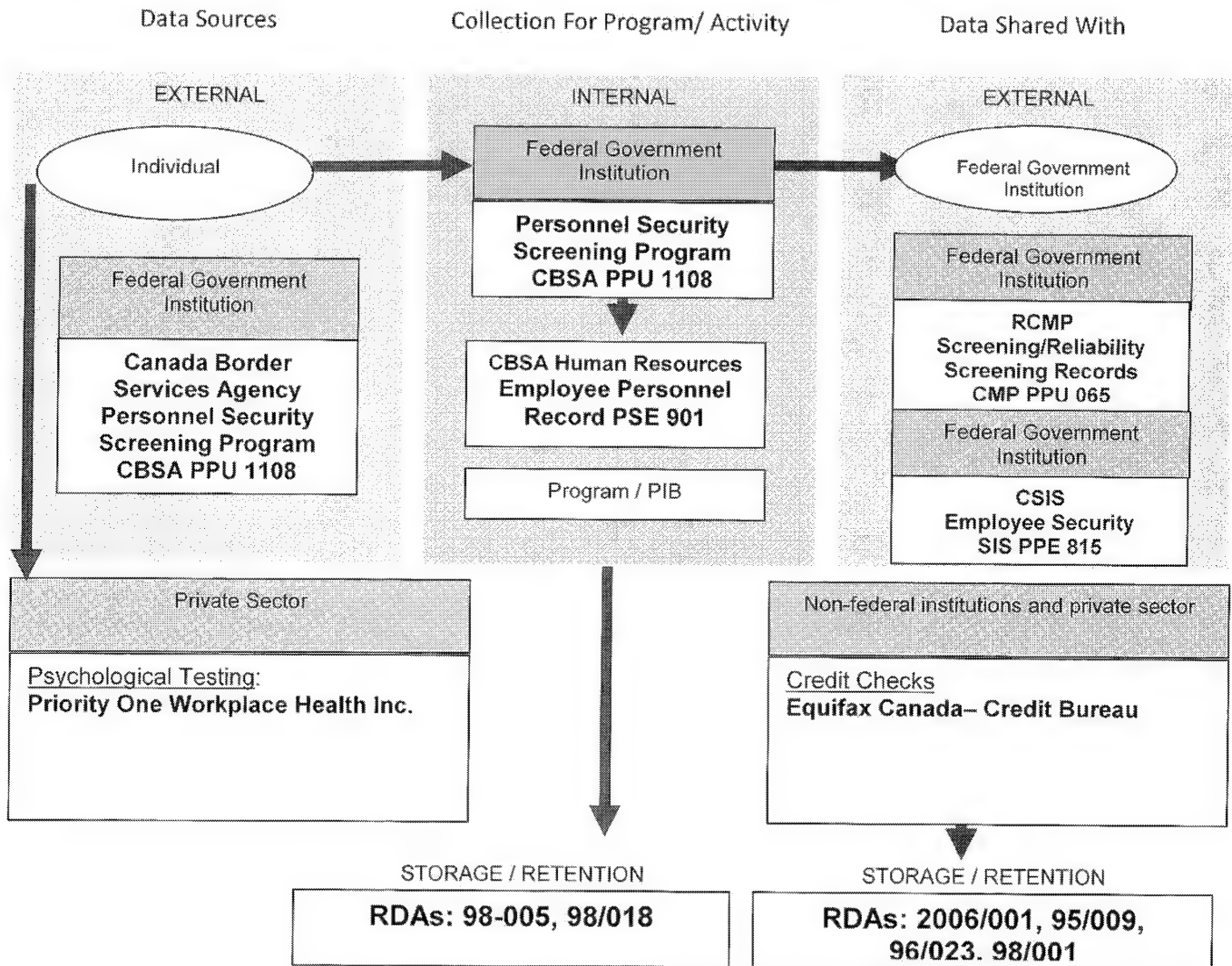
PIA

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
	If any person is deceased, date of death and last address is to be included.			
Friends/Colleagues	Character References/ Neighbourhood Reference	First & Last Name / Relationship / Dates Known For / Complete Home Address / Telephone Numbers	Paper Form: <u>TBS 330-60</u>	To asses reliability status/loyalty.
Criminal Justice	Criminal Convictions	Criminal convictions details (if applicable) / Charge(s) / Name of Convicting Police Force / Date of Conviction	Paper Forms: <u>TBS 330-23</u> <u>TBS 330-60</u>	To asses reliability status/loyalty.
Employment	Current/Historical (10 yrs) Employment Information	Name of Employer / Supervisor Name / Dates Employed / Job Title / Employer Address / Supervisor Telephone Number	Paper Form: <u>TBS 330-60</u>	To asses reliability status/loyalty.
Employment	Foreign Employment/Assets	Free Text Details of Foreign Employment / Free Text Details of Foreign Assets	Paper Form: <u>TBS 330-60</u>	To asses reliability status/loyalty.
Travel	Travel	Country / Travel Purpose (free text field) / Dates Traveled	Paper Form: <u>TBS 330-60</u>	To asses reliability status/loyalty.
Education	Education	Last School Attended Name / Student ID Number / Location of School / Dates Attended / Field of Study-Diploma Received	Paper Form: <u>TBS 330-60</u>	To asses reliability status/loyalty.
Other	Signature	Signature	Paper Form: <u>TBS 330-23</u> <u>TBS 330-60</u>	To validate/authorize information provided on forms.

SECTION 4 - FLOW OF PERSONAL INFORMATION

Identify the flow of the personal information within and outside the institution's program or activity. Institutions may choose to outline the flow of personal information in the format of their choice.

4.1 Example of a Data Flow Model – Diagram - **SEE ANNEX 6 FOR DETAILED DATA FLOW**



4.2 Example of a Data Flow Model - Table

Source of the personal information for the program or activity

From whom or from what organization is the personal information collected. In other words, identify who is providing the personal information that is being used, will be used or available for use for the program or activity. There may be more than one source, indicate all sources:

SOURCE	IDENTIFY THE SOURCE
The individual seeking Employment	Any individual seeking employment at Canada Border Services Agency (CBSA)
A federal government institution (identify from what PIB the information is obtained)	Royal Canadian Mounted Police (RCMP) – Screening/Reliability Screening Records CMP PPU 065 Canadian Security Intelligence Service (CSIS) – Employee Security SIS PPE 815
Non federal institutions	
- Provincial Government	
- Municipal Government	
- Aboriginal Government/ Council	
- Organization of a Foreign State	
- International Organization	
Private Sector	
- Located in Canada and Canadian Owned	Psychological Testing: Priority One Workplace Health Inc. (Previously submitted annex 8)
- Located in Canada and Foreign Owned	Credit Bureau Checks: Equifax Canada– Credit Bureau (Previously submitted annex 12 contains a Handling of Personal Information Section) All transmission and servers are located in Canada. The only instance where tombstone data may be disclosed to the US is where we are clearing a US resident (rare).
- Located abroad and Canadian Owned	
- Located abroad and Foreign Owned	

4.3 Internal Use and Disclosure

Where will that information circulate within the federal government institution? This must identify any related programs or activities and personal information banks as identified in the institution's Info Source chapter.

Program	Personal Information Bank
Personnel Security Screening Program	Personnel Security Screening Program CBSA PPU 1108
CBSA Human Resources	Employee Personnel Record PSE 901

4.4 External Use and Disclosure

Where will that information circulate outside of the federal government institution? This includes any disclosure made to:

The individual or a representative	
A federal government institution	Royal Canadian Mounted Police (RCMP) – Screening/Reliability Screening Records Canadian Security Intelligence Service (CSIS) – Employee Security
Non-federal institutions and private sector	
- Provincial Government	
- Municipal Government	
- Aboriginal Government/ Council	
- Organization of a Foreign State	
- International Organization	
Private Sector	
- Located in Canada and Canadian Owned	Psychological Testing: Priority One Workplace Health Inc.
- Located in Canada and Foreign Owned	Credit Bureau Checks: Equifax Canada– Credit Bureau (Previously submitted annex 12 contains a Handling of Personal Information Section) All transmission and servers are located in Canada. The only instance where tombstone data may be disclosed to the US is where we are clearing a US resident (rare).
- Located abroad and Canadian Owned	
- Located abroad and Foreign Owned	

4.5 Retention / Storage

Where will the information be stored or retained (identify all organizations that will store the information – this includes duplicates of the databases containing the personal information or any back-ups):

A federal government institution	Canada Border Services Agency (CBSA) – RDA 98-005 Royal Canadian Mounted Police (RCMP) – RDA 95/009, 96/023, 98/001 Canadian Security Intelligence Service (CSIS) – RDA 2006/001
Federal Government Systems	Automated Personnel Security Screening System (APSS) (Previously submitted annex 2 and 10) Professional Standards Case Management System (PSCMS) (previously submitted Annex 9) CBSA RDA Number: 98-005

Name of Program / Activity / Service	PIA
A Federal Records Centre	Canada Border Services Agency (CBSA) – RDA 98-005 Royal Canadian Mounted Police (RCMP) – RDA 95/009, 96/023, 98/001 Canadian Security Intelligence Service (CSIS) – RDA 2006/001
Non federal institutions and private sector	
- Provincial Government	
- Municipal Government	
- Aboriginal Government/ Council	
- Organization of a Foreign State	
- International Organization	
Private Sector	
- Located in Canada and Canadian Owned	Psychological Testing: Priority One Workplace Health Inc. Storage location has been security cleared through the Canadian Industrial Security Directorate (CISD) of the Public Works and Government Services of Canada (PWGSC) to the level of PROTECTED B as outlined in the Dr. Barker - EP537-060013 Contract .(Previously submitted annex 8)
- Located in Canada and Foreign Owned	Credit Bureau Checks: Equifax Canada– Credit Bureau (previously submitted Annex 12 contains a Handling of Personal Information Section) All transmission and servers are located in Canada. The only instance where tombstone data may be disclosed to the US is where we are clearing a US resident (rare).
- Located abroad and Canadian Owned	
- Located abroad and Foreign Owned	

4.6 Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

Identify the areas / groups / divisions who are allowed to access and handle the personal information collected for the program or activity. Also, identify where these areas or groups are located (i.e. national capital region, within a province, in a foreign country, or several locations if tele-working) as well as the location of the personal information to uncover any potential trans-border or inter-jurisdictional issues. Where reasonable to do so, by virtue of the size of the organization or the number of individuals, identify individual positions rather than the work area or group.

Federal government Institution responsible for program or activity:

Canada Border Services Agency

Name of Program / Activity / Service		PIA
Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
Canada Border Services Agency (CBSA) – Personnel Security Screening Program	- Employees in the Security & Professional Standards Directorate, Personnel Security Screening Program - Approximately 16 people (based on business needs the numbers may change as required).	National Capital Region
Other federal government Institution responsible for program or activity: (one table per institution):		
Royal Canadian Mounted Police (RCMP)	-Employees in the Security Intelligence Background Section assigned to work on CBSA files -Approximately 6 people (based on business needs the numbers may change as required).	National Capital Region
Canadian Security Intelligence Service (CSIS)	Security Screening Branch	National Capital Region
Non Federal Institution or Private Sector: 'name': (one table per institution)		
Priority One Workplace Health Inc.	- Psychologists working for the said company who conduct the psychological test and interview as well as the Head Psychologist of the organization.	Calgary, AB – Head Quarters Saint-John, NB Quebec, QC Montreal, QC National Capital Region Toronto, ON Niagara Falls, ON Windsor, ON Sault-Ste. Marie, ON Winnipeg, MB Regina, SK Vancouver, BC

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority for Collection of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes

- 1.1 ☒ Please specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Section 7, 11.1(1) and 12(1)(e) of the Financial Administration Act, Sections 5 and 11 of the Canada Border Services Agency Act and Section 31 of the Public Service Employment Act for

Name of Program / Activity / Service

PIA

security screening purposes.

- 1.2 ☒ AND, ensure that the legal authority to collect the personal information is cited in the relevant PIB and in "Section 1 – Overview and PIA Initiation" of the core PIA.

→ Continue to Question 2

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your institution's legal advisors to determine if there is authority to proceed with the program or activity.

2. Necessity to Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.
- 2.2 ☒ AND, implement controls and procedures to ensure the institution does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

→ Continue to Question 3

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority for the Collection, Use or Disclosure of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):
- 3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

3.3 ☐ Establish explicit authority through legislative amendment(s).

3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the institution is to occur on a routine or systematic basis

3.4.1 ☐ To another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

3.5 ☐ AND, ensure that the relevant PIB for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ Continue to Question 4

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ Continue to Question 4

4. Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and section 6.1.2 and 6.4.1 of *Directive on Social Insurance Number*

YES

4.1 ☒ A "Privacy Notice" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must notify the individual of any of the following elements that apply (please check all appropriate boxes):

☒ a) The purpose and authority for the collection

☒ b) Any uses or disclosures that are consistent with the original purpose.

☐ c) Any uses or disclosures that are not related to the original purpose.

☒ d) Any legal or administrative consequences for refusing to provide the personal information

☒ e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.

☒ f) A reference to the PIB for the program or activity

☐ g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "Consent Statement" to the "Privacy Notice" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose or a consistent use, or, to authorize indirect collection of personal information.

4.2 ☒ The "Consent Statement" must include, as applicable, the following elements (please check all appropriate boxes):

☒ a) The purpose of the consent and the specific personal information involved.

Name of Program / Activity / Service

PIA

- ☒ b) In the case of indirect collections, the sources that will be asked to provide the information.
- ☒ c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
- ☒ d) Any consequences that may result from withholding consent.
- ☐ e) Any alternatives to providing consent

4.3 ☒ AND, implement controls and procedures to ensure that the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

→ Continue to Question 5

NO

4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the institution, or from another institution, government or third party.

→ Continue to Question 5

5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*. **Policy reference:** Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

the Privacy Regulations?

YES

5.1 ☒ The notice and consent requirements stated at Question 4 apply. Please review the required elements listed under "YES" at Question 4 and check the corresponding boxes below to indicate the elements that need to be included in the "**Privacy Notice**" or the "**Consent Statement**" (check all that apply):

Privacy Notice	a) <input checked="" type="checkbox"/>	b) <input checked="" type="checkbox"/>	c) <input type="checkbox"/>	d) <input checked="" type="checkbox"/>	e) <input checked="" type="checkbox"/>	f) <input checked="" type="checkbox"/>	g) <input type="checkbox"/>
Consent Statement	a) <input checked="" type="checkbox"/>	b) <input checked="" type="checkbox"/>	c) <input checked="" type="checkbox"/>	d) <input checked="" type="checkbox"/>	e) <input type="checkbox"/>		

5.2 ☒ AND, implement controls and procedures to ensure the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

→ Continue to Question 6

NO

5.4 ☐ → Continue to Question 6

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the *Policy on Privacy Protection* and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

☐ a) The collection is a result of a disclosure to the institution under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided:

☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates.

6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant PIB.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a core PIA for the program or activity has been adequately documented in the description of the program or activity in "Section 1 - Overview and PIA Initiation" of the core PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "Privacy Notice" or the "Consent Statement" includes all of the required elements listed under "YES" at Question 4.

→ Continue to Question 7

NO

6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).

→ Continue to Question 7

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:

Retention and Disposal Standards: Records will be retained for 2 years after an employee has left Canada Border Services Agency (CBSA) and then records are destroyed. If a security clearance is revoked, records will be retained for 5 years and then destroyed.

RDA Number: 98-005

- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.
- 7.3 ☒ AND, if the institution intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.
- 7.4 ☒ AND, the institution must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

→ Continue to Question 8

NO

- 7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.
- 7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the institution, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- 7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

→ Continue to Question 8

8. Accuracy Of Personal Information

Will measures be adopted to ensure that personal information used by the institution for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the institution) where this is authorized, or where consent was obtained. Please briefly describe the data-matching process and the source(s) that will be used to ensure accuracy of the information:

Data matching activities take place with our HIPSSS partners – RCMP, and CSIS – in order to validate and substantiate information provided by individuals being subjected to the CBSA Personnel Security Screening process.

8.1.3 ☐ In cases where direct collection or consent is not feasible, the institution will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use. Please identify the sources and procedures to be used to check the accuracy of the information:

8.1.4 ☐ Technological methods will be used to identify errors and discrepancies. Please briefly describe these technological methods:

8.1.5 ☒ Other – please specify:

The most important aspect of the screening process is to establish the accuracy (reliability) of personal information. This is conducted by verifying Information from a variety of sources and cross referencing the information/documents collected to support the screening. The sources include but are not necessarily limited to:

Originating Agencies

Personnel Screening Consent & Authorization Form - TBS 330-23 (Previously submitted annex 14)

Integrity interview

Digital Fingerprints

CSIS & RCMP Background Checks

Criminal Records Checks/Background Checks/Enforcement Database Checks

Proof of biographical data – diplomas, birth certificates

Reference Checks

Open Source Checks

8.2 ☐ AND, if measures are adopted other than "direct collection or validation with the individual or with a person authorized to act on behalf of the individual", the institution must implement appropriate controls and procedures to ensure that:

a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;

Name of Program / Activity / Service

PIA

- b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
- c) personal information can only be modified or corrected by those within the institution who have the authority to do so; and
- d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the institution are corrected / annotated.

8.3 ☒ AND, if appropriate, ensure that the "**Privacy Notice**" or "**Consent Statement**" and the relevant PIB are amended to identify the data-matching activity including the source(s).

→ Continue to Question 9

NO

8.4 ☐ Please explain why such measures will not be adopted:

→ Continue to next Question 9

9. Use Of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties.
- 9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "*Section 4 – Flow of Personal Information*" of the core PIA identify the areas, groups and individuals (e.g., the positions) within the institution who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.
- 9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the institution will adhere to the requirements and principles in its "**Privacy Protocol For Non-Administrative Purposes**", in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

→ Continue to Question 10

NO

9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are

Name of Program / Activity / Service

PIA

not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the institution pursuant to subsection 8(2) of the *Privacy Act*:

- 9.5 ☐ AND, ensure that these other uses are reflected in the relevant PIB.
- 9.6 ☐ AND, include a description of these other uses in the "**Privacy Notice**" or "**Consent Statement**", as appropriate,
- ☐ AND, ensure the all the other applicable requirements listed under "**YES**" at Question 9 are met.
- Continue to Question 10

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*)

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the institution, please identify the branch and the program or activity.

- 10.1.1 ☒ Within the institution for another program or activity – specify

The security screening status may be shared with the CBSA Human Resources officials to update the individual's personnel file - refer to Standard Personal Information Bank Employee Personnel Record (PSE 901).

- 10.1.2 ☒ Other federal government institutions – specify

Information may be shared with the Canadian Security Intelligence Service (CSIS), Security Assessments/Advice (SIS PPU 005) and the Royal Canadian Mounted Police (RCMP), Forensic Science and Identification Services and Canadian Criminal Real Time Identification Services (CMP PPU 030 005), as service providers in accordance with the Policy on Government Security and the Royal Canadian Mounted Police (RCMP), Operational Case Records (CMP PPU 005) for database checks. It may also be shared with other government departments (OGDs) to confirm security screening status.

The Privacy Act Statement (below) from the 330-23 (previously submitted Annex 14) outlines the authority to collect information. The information on this form is required for the purpose of providing a security screening assessment. It is collected under the authority of subsection 7(1) of the Financial Administration Act and the Policy on Government Security (PGS) of the Government of Canada, and is protected by the provisions of the Privacy Act in institutions that are covered by the Privacy Act. Its

collection is mandatory. A refusal to provide information will lead to a review of whether the person is eligible to hold the position or perform the contract that is associated with this Personnel Screening Request. Depending on the level of security screening required, the information collected by the government institution may be disclosed to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS), which conduct the requisite checks and/or investigation in accordance with the PGS and to entities outside the federal government (e.g. credit bureaus). It is used to support decisions on individuals working or applying to work through appointment, assignment or contract, transfers or promotions. It may also be used in the context of updating, or reviewing for cause, the reliability status, security clearance or site access, all of which may lead to a re-assessment of the applicable type of security screening. Information collected by the government institution, and information gathered from the requisite checks and/or investigation, may be used to support decisions, which may lead to discipline and/or termination of employment or contractual agreements. The personal information collected is described in Standard PIB PSU 917 (Personnel Security Screening) which is used by all government agencies, except the Department of National Defence PIB DND/PPE 834 (Personnel Security Investigation File), RCMP PIB CMP PPU 065 (Security/Reliability Screening Records), CSIS PIB SIS PPE 815 (Employee Security), and PWGSC PIB PWGSC PPU 015 (Personnel Clearance and Reliability Records) used for Canadian Industry Personnel. Personal information related to security assessments is also described in the CSIS PIB SIS PPU 005 (Security Assessments/Advice). We also currently have a signed Letter of Intent with the RCMP and are currently in discussions with the RCMP to finalize the details of the corresponding MOU.

10.1.3 ☒ Provincial, territorial or municipal governments institutions – specify

Information relating to the commission of criminal offences will be disclosed to accredited domestic law enforcement agencies in the administration or enforcement of the law and in the detection, prevention or suppression of a crime.

10.1.4 ☐ Foreign government institutions and entities thereof – specify

10.1.5 ☐ International organizations – specify

10.1.6 ☒ The private sector (e.g., contractor or other external service provider) – specify

Information may be shared with entities outside the federal government, including credit bureaus. However, this is limited to name, date of birth, and address. (Previously submitted annex 12)
Psychological Testing - Priority One Workplace Health Inc. (Annex 8)

10.1.7 ☐ Other – specify

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant PIB in *Info Source*, including the specific purpose of the disclosure;
- f) the "Privacy Notice" or "Consent Statement" describes any disclosures of information; and,
- g) the "Data Flow Diagram" or "Data Flow Tables" completed in "Section 4 – Flow of Personal Information" of the core PIA include details on the disclosed personal information:

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or trans-border flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
- f) Obligations are to be extended to other parties such as subcontractors.

→ Continue to Question 11

NO

10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

→ Continue to Question 11

11. Accounting For New Uses or Disclosures Not Reported in Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in Info Source?

Statutory reference: Sections 7 to 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.9 and 6.2.2 of *Directive on Privacy Practices*

Name of Program / Activity / Service

PIA

YES

- 11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:
- a) the head of the institution or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *Info Source*;
 - b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified forthwith regarding the new consistent use;
 - c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *Info Source* will only be made with the consent of the individual to whom the information relates;
 - d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure;
 - e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;
 - f) the Privacy Commissioner is notified forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant PIB published in *Info Source*;
 - g) the relevant PIB is amended in time for the next edition of *Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and
 - h) the Privacy Commissioner is notified prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
 - i) Other, specify

→ Continue to Question 12

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented (provide adequate justification):

→ Continue to Question 12

12. Safeguards - Statement Of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of

the personal information to be collected and retained for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the core PIA.

The CBSA Statement of Sensitivity (previously submitted Annex 2) was conducted on the Agency Personnel Screening System (APSS) and all recommendations were applied. It should be noted that a Statement of Sensitivity will also be performed on the IA Pro is now being referred to as Professional Standards Case Management System (PSCMS). In the interim, we have provided (previously submitted Annex 9) IA Pro (PSCMS)-Service Level Agreement which offers some detail about the system.

→ Continue to Question 13

NO

- 12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

→ Continue to Question 13

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 13.1 ☒ Reference the title of the TRA or other security assessment in "Section 6 - Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Previously submitted Annex 1_Threat Risk Assessment (TRA) PerSec Room 9th FI_final - this TRA was to assess the Personal Security Screening File Room floor space against physical security standards for the increased holding of Protected B information.

Previously submitted Annex 11_HIPSS Physical Security TRA Review -The May 2012 PIA was reviewed to determine if additional physical security safeguards were required to support the new High-Integrity Security Screening Standard.

Name of Program / Activity / Service	PIA
--------------------------------------	-----

13.2 ☒ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

13.3 ☒ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*.

→ Continue to Question 14

NO

13.4 ☐ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

→ Continue to Question 14

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information (see **PIA Action Plan**)
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches
- ☒ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other – please describe

14.2 Physical safeguards

- ☒ Restricted access areas

- ☐ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☒ Combination locks
- ☐ Safes
- ☐ Cipher locks
- ☐ Key cards
- ☐ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☒ Other – please describe

(previously submitted Annex 1) Threat Risk Assessment PerSec Room 9th FI and the (previously submitted Annex 11) HIPSSS Physical Security TRA Review were conducted to ensure the physical safeguarding of information.

All recommendations were applied.

CBSA does have strong safeguards in place for the storage of personal information related to the HIPSSS. The safeguarding procedures have been consolidated in previously submitted Annex 3.

Additional security measures have also been put in place for the Personnel Security Screening file room (previously submitted Annex 4).

14.3 Technical safeguards

- ☐ Role-based user authorization and authentication
- ☐ Biometrics
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☒ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☒ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☐ Intrusion Detection System (IDS)
- ☐ Virtual Private Network (VPN)
- ☒ Encryption of sensitive information
- ☒ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☒ Audit trails
- ☒ Other – please describe

(previously submitted Annex 10) Agency Personnel Security Screening APSS TRA and (previously submitted Annex 2) Agency Personnel Security Screening APSS Statement of

Name of Program / Activity / Service

PIA

Sensitivity were conducted to ensure the safeguarding of information contained in IT systems.
 All recommendations were applied.
 CBSA does have strong safeguards in place for the storage of personal information related to HIPSSS. The safeguarding procedures have been consolidated in previously submitted Annex 3.

→ Continue to Question 15

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

Statutory reference: Sections 4 to 10 of the Privacy Act and section 4 of Privacy Regulations

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of Directive on Privacy Practices

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the core PIA;
- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant PIB and in "Section 3 – Analysis of Personal Information Elements" of the core PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

→ Continue to Question 16

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.

→ Continue to Question 16

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

Name of Program / Activity / Service

PIA

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "*Section 2 – Risk Area Identification and Categorization*" of the core PIA.
- 16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant PIB and in *Section 3 – Analysis of Personal Information Elements* of the core PIA.
- 16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.

☐ If notice about surveillance or monitoring will not be provided, please explain why:

- 16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

→ Continue to Question 17

NO

- 16.6 ☒ The new or modified program or activity will not result in surveillance or monitoring.

→ Continue to Question 17

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 17.1 ☐ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 17.2 ☐ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

- 17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it

Name of Program / Activity / Service	PIA
<p>is adequately reflected in the response to Question 1 of "<i>Section 5 – Privacy Compliance Analysis</i>" and in "<i>Section 1 – Overview and PIA Initiation</i>" of the core PIA.</p> <p>17.4 <input type="checkbox"/> AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant PIB and in "<i>Section 3 – Analysis of Personal Information Elements</i>" of the core PIA.</p> <p>17.5 <input type="checkbox"/> AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.</p> <p><input type="checkbox"/> If notice about the compliance/regulatory investigation or law enforcement activities will not be provided, please explain why:</p> <div data-bbox="319 689 1417 788" style="border: 1px solid black; height: 44px; margin-top: 5px;"></div> <p>NO</p> <p>17.6 <input checked="" type="checkbox"/> The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.</p>	

Name of Program / Activity / Service

PIA

Note: The table below can be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	(Examples) Legal authority for the program has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program have been carefully assessed based, for example, on the institution's experience gained with the administration of a similar program. The personal data collected will be limited to only what is required. b) These categories and elements of personal information have been described in the relevant PIB for the program. c) Controls and procedures will be implemented to ensure that the institution does not collect more personal information than necessary for the program and that a continuing need exists for that information and its collection.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements may be included here.) b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i> .	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
7	a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program. b) Controls and procedures have been implemented within the program and the ATIP Office to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the Privacy Regulations. c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

SECTION 6 - Summary of Analysis and Recommendations

1. Type of Program or Activity: Personnel Security Screening - Personal information is used to support decisions for granting, denying, revoking or reviewing for cause the reliability status, security clearance or site access of individuals working or applying to work through appointment, assignment or contract at the Canada Border Services Agency (CBSA).

Program or Activity Partners and Private Sector Involvement: With other federal government departments, accredited domestic law enforcement agencies and private sector organizations – *Priority One Workplace Health Inc.* and *Equifax Canada*.

Privacy risk:

The CBSA will share personal information externally with its Personnel Security Screening partners: Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS) for the purpose of conducting reliability personnel security screening checks, conducting database checks, periodic data matching and to assess an individual's reliability and reliability as it relates to loyalty.

Mitigation:

The disclosure of personnel security screening information (including third party information is managed on a case-by-case basis and any request for personnel screening information that has not already been pre-authorized (e.g. sharing of screening status with OGDs, HR at the CBSA, or to the RCMP and CSIS as mandated by PGS) is to be directed to the manager for guidance and approval.

A disclosure form has been specifically developed to support disclosures of information collected for screening purposes.

A Memorandum of Understanding (MOU) is being finalized with the CBSA Personnel Security Screening partner RCMP to ensure both parties are properly storing, caring for, using and disclosing personal information. With respect to CBSA's other Personnel Security Screening partner Canadian Security Intelligence Service (CSIS), the Treasury Board *Policy on Government Security and Personnel Security Standard* defines their authority and role as it relates to the sharing of personal information related to the CBSA Personnel Security Screening Program. Personal information will not be disclosed for any purpose other than the purpose (including consistent uses) for which it was originally collected.

All disclosures of Personnel Security Screening information must be made in accordance with the provisions of the *Privacy Act*, *Sections 5 and 11 of the Canada Border Services Agency Act*, *Section 31 of the Public Service Employment Act*, *Customs Act*, *Access to Information Act*, the *Canada Border Services Agency (CBSA) Departmental Security Policy* and/or the *Policy on Government Security*. In the case of private sector involvement, personal information is collected directly by the CBSA approved vendor (private sector psychologist). Any personal information pertaining to the candidate, tests questions and answer sheets, the candidate's responses, and the interview with the psychologist are kept confidential and not provided to

CBSA. The only information provided to the CBSA by *Priority One Workplace Health Inc.* is the result of an employee's "suitability" or "unsuitability".

With respect to the contract with *Priority One Workplace Health Inc.*, all test materials must be immediately shipped upon completion to the Contractor's identified main holding location (main "Hub"). No completed materials are to remain in the Contractor's satellite locations. All information held at the main "Hub" that will be identified to the CBSA. This location has been security cleared through the *Canadian Industrial Security Directorate (CISD)*, *Public Works and Government Services Canada (PWGSC)* to the level of **PROTECTED B** as specified in Annex 8.

During the period of the Contract, the Contractor must collect, store, handle, and maintain all original materials, including test sheets, interview questions, reports, and notes pertaining to current and future CBSA personnel.

On completion of the Contract, the Contractor must retain all materials, including test sheets, interview questions, reports, and notes pertaining to current and future CBSA personnel in a manner consistent with the standards set forth by their professional governing body (i.e. the College of Psychologists of British Columbia) and the *Canadian Code of Ethics for Psychologists. If the standard set by the provincial authority is less than five (5) years the Contractor must retain all current and future CBSA personnel materials for a period of 5 years from current and future CBSA personnel test date. After the retention period, with the consent of the Project Authority, all materials pertaining to the current and future CBSA personnel, must be destroyed as per standards set forth by their professional governing body.

***Canadian Code of Ethics for Psychologists**

2. Type of Personal Information Involved and Context: Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.

Privacy risk:

The CBSA collects a wide variety of personal information through its activities. Personnel Security Screening information may contain detailed personal information such as occupation, annual salary, criminal sexual behaviour, criminal history, and past drug use. In order to fulfill CBSA's mandate of ensuring the security and prosperity of Canada by managing access of people and goods to and from Canada, CBSA must ensure that all its employees conduct themselves with integrity, respect and professionalism. In order to achieve this, CBSA must collect and analyze sensitive personal information as an integral part of the Personnel Security Screening Process.

Necessity

The purpose of the Integrity interview (using the Integrity Interview Guide) is to validate information that may be obtained through database checks and other sources. It will also identify if the applicant has been honest and truthful when responding to the questions, which is a fundamental requirement for obtaining a Reliability Status. Refer to the previously submitted Annex 6_IQ Justification Preamble; the previously submitted Annex 7_IQ Justification chart and the new Annex 33 Justification for the Questions in the Integrity Interview Guide for

Name of Program / Activity / Service	PIA
--------------------------------------	-----

more information about why the inclusion of privacy invasive questions are required for the HIPSSS. Not only have the questions been reviewed but also their application. .

The HIPSSS will ensure that all CBSA employees, regardless of position, would be rigorously screened at the time of determining their Reliability status prior to an offer of employment and during the renewal process (pursuant to the TBS Personnel Security Standard), in order to uphold the public's trust and reduce the Agency's vulnerability to fraud, infiltration and corruption. It should be noted that the Security Screening under the HIPSSS will only be conducted when an individual is successful in the staffing process and is selected for appointment into a position, or where a pool is established for eventual appointment. Security Screening is one of the conditions of employment that must be satisfied before an appointment is finalized.

The added screening tools under the HIPSSS will significantly minimize the potential security risks and further enhance program integrity. All individuals would be security screened to at least the same level or higher than that the membership to the various internal CBSA programs such as NEXUS, FAST, CANPASS, etc. (see the previously submitted case studies (Annex 22) and the Employee Misconduct Risk Assessment (previously submitted Annex 21) as further examples of the significant risks for corruption, fraud and criminal interference in the CBSA

Effectiveness

The CBSA has established criteria to evaluate the effectiveness of the HIPSSS program.

A review of the Integrity Questionnaire has been completed in an effort to:

- ensure that the questions are targeted directly at the individual whose security and integrity needs to be verified
- avoid misunderstanding and minimize the potential over-collection of information not directly relevant to HIPSSS.

Feedback on the Integrity Questionnaire has been analyzed. As such, the questions were modified and the questionnaire is now used as a reference guide in the conduct of an Integrity interview and not as a stand-alone questionnaire that an individual must complete in writing and submit to the CBSA. The questions were modified to include the following changes: certain questions were amended to request information for a three year timeframe; requests for information regarding a "spouse/common law partner or cohabiter" were removed due to privacy, consent and/or concerns of discrimination on the basis of family or marital status; questions related to criminal activity were revised to request only information related to charges or convictions thereby eliminating the possibility of self-incrimination; and certain questions were eliminated since the information requested was irrelevant.

A review of the application of the Integrity interview with the use of the Integrity Questionnaire as a reference guide has also been completed and it has been determined that at this time, it will not apply to current employees of the CBSA or individuals who already have valid government security screening from another Federal Government Department unless there is adverse security information about the individual. The Integrity interview, which pre-existed the HIPSSS under the TBS Policy on Government Security, will be used for new Border Services

Name of Program / Activity / Service	PIA
--------------------------------------	-----

Officers, and other new employees to the CBSA who do not have an existing Government of Canada Security Screening.

Mandatory reporting is required through the Functional Management Model (FMM). The FMM was introduced in 2009-2010 to improve national program consistency as part of the Agency's Change Agenda. It is a new approach to program management that links resource allocations to program performance and risk, enhancing our ability to understand, monitor and control the costs and performance of all programs. Details of the FMM reporting requirements can be found in Annex 20.

We are currently preparing a checklist which will be used for sampling purposes on a daily basis by senior analysts and for post analysis of the files processed through HIPSSS to ensure:

- the information is being used consistently for the purposes that it was collected;
- the proper screening decisions have been rendered;
- no unlawful disclosure of personal information has occurred; and
- the established level of authority for granting, denying and/or revoking was respected.

This will help ensure the effectiveness of the HIPSSS program.

Additional criteria may be established after the full program review/reporting and adjustment in Phase 3, as required.

In addition, we have prepared the following documents to address the concerns identified in the OPC's review of the initial HIPSSS PIA that was submitted in May 2012:

- Previously submitted Annex 18 The Privacy Four Part Test; and
- Previously submitted Annex 17 The Privacy Risks.

Proportionality:

The implementation process for the HIPSSS and the Integrity interview (using the Integrity Interview Guide) will be clearly outlined in communications products.

Anyone requiring a CBSA security screening will be screened through the HIPSSS. This includes all CBSA employees (permanent, term, casual, and part-time), contract and private agency personnel, and individuals seconded or assigned to CBSA (including students). Security screening requirements are identified as a condition of employment or an agreement (i.e. written collaborative arrangement or agreement).

- In addition to the baseline verifications of employment history, credit and criminal record checks that are currently being conducted, individuals who are not employees and individuals who are being considered for employment with the CBSA will also undergo the following verifications:
 - Law Enforcement Record Checks
 - Internal data base checks
 - Integrity interviews
 - Other checks may be undertaken for cause on a case by case basis.

Name of Program / Activity / Service	PIA
--------------------------------------	-----

- All individuals, upon renewal or upgrade to their CBSA security screenings will undergo the following verifications:
 - Law Enforcement Record Checks
 - Internal data base checks
 - Integrity interviews (for cause)
 - Other checks may be undertaken for cause on a case by case basis.
- In addition, all armed officers who do not hold a valid Possession and Acquisition Licence (PAL) or who have not yet been screened through the HIPSSS, will be screened through the HIPSSS in advance of their normal renewal cycle.

However, it should be noted that at this time, only new Border Services Officers and other applicants to the CBSA who do not hold a valid Security Screening issued by a Federal Government Department will be subjected to a Integrity interview with the use of the Integrity Questionnaire as a reference guide as part of the HIPSSS process. However, an employee may be asked to participate in an Integrity Interview to assess their integrity or if the CBSA has obtained or uncovered information that places his/her security screening status in question.

Minimization

To minimize the intrusiveness of the HIPSSS, the OPC had suggested that CBSA should consider the least invasive means of effectively conducting security screening. The HIPSSS process includes a variety of reviews and checks in order to determine the integrity and reliability of a potential CBSA employee. In addition to the current checks which include criminal records check, credit check, fingerprint collection, residential and travel history, CSIS indices check, employment and education verification and an interview, HIPSSS will also subject all current and potential CBSA employees to screening against additional Royal Canadian Mounted Police (RCMP) databases, CBSA enforcement database checks and could potentially include a psychological evaluation (for cause).

While the many checks administered through the HIPSSS appear to cover similar ground, they are necessary to validate the information and to validate the integrity and honesty of the individual.

The written Questionnaire has been replaced with Integrity Interviews and the questions from the Questionnaire were modified based on consultation with the OPC and other stakeholder and used to develop an Integrity Interview Guide, henceforth referred to as the Guide. The Guide is used in the conduct of Integrity interviews of new Border Services Officer recruits and for the recruitment of other individuals coming to work at the CBSA. An Integrity interview could be required to assess an existing employee's integrity or if information is brought forward that questions the person's qualification for security screening. We deem that it is necessary to obtain as much information as possible from individuals for whom the Government of Canada does not have any background information. The multi-faceted role of the CBSA has created the need for a higher degree of integrity among staff than for other departments and agencies. Many aspects of the CBSA's work are vulnerable to corruption, fraud or infiltration by the criminal element, particularly since the CBSA has access to sensitive information and monopoly power over certain services, such as the release of cargo and conveyances and the clearance of

Name of Program / Activity / Service	PIA
--------------------------------------	-----

passengers into Canada. If coerced by the criminal element, the CBSA's ability to provide effective integrated border services could be compromised. It could also impact public safety, public trust, relationships with domestic and international partners, and the economic well-being of the country and national security.

Sensitive law enforcement, national security, immigration, and customs information related to these responsibilities is held on information systems within the Agency. The majority of CBSA employees have access to these systems to some degree and therefore their integrity must be beyond reproach. Implementing the HIPSSS would allow for an in-depth, global assessment of all individuals working within the CBSA, as well as candidates applying to work for the CBSA, to ensure the Agency is further protected against fraud, infiltration and corruption. It should not be forgotten that the CBSA is following the lead of other Federal Government "Enforcement" Departments Security screening programs where their employees have similar responsibilities to protect Canadian Society.

The CBSA received TB approval to implement the following assessment tools within the reliability status security screening process:

1. To utilize an Integrity Questionnaire, which has been discontinued. However, modified questions have been used to develop the Integrity Interview Guide which is in the conduct of Integrity interviews;
2. To conduct an integrity interview;
3. To query the CBSA enforcement databases with Customs and Immigration information;
4. To query the Royal Canadian Mounted Police (RCMP) databases for Law Enforcement Record Checks;
5. To query the Citizenship and Immigration Canada (CIC) enforcement databases, which has not been implemented;
6. To administer a psychological test to further assess ethical behaviour, integrity and honesty of candidates where required.

Mitigation:

Under the PGS and Financial Administration Act, Sections 7(1), 11.1(1) and 12(1) (e), we have the authority to collect and retain information if it is used to support a personnel screening decision.

The majority of the personal information collected has a security classification of Protected B and each person's information is generally of a detailed personal nature. As such, all personal information, regardless of storage medium, must be stored either in a locked cabinet (or container or a safe) or in a secure room designed in accordance with specifications approved by the Security and Professional Standards Directorate's Personnel Security Screening Program of the CBSA – see previously submitted Annex 1_Threat Risk Assessment (TRA) PerSec Room 9th Floor and Annex 11_HIPSS Physical Security TRA Review and the Instructions contained within previously submitted Annex 5 - Integrity Questionnaire.

All retention and disposal of personal information will be carried out in accordance with the relevant retention and disposal standards as defined by *Library and Archives Canada* in cooperation with the CBSA – see **Personal Information Bank for Retention and Disposal Standards details**.

The safeguarding measures to protect the retention, destruction and disclosure of information are identified in previously submitted Annex 3. Included in this annex is a copy the Disclosure Authorization Form for Personnel Security Screening. The form entitled "Provision/Access and Use of Personnel Security Information" (in accordance with the Policy on Government Security) has been developed to record the provision, access, and use of personal information collected for the purposes of personnel screening by the CBSA.

It should be noted that the information that is being provided to our partners to support screening is minimal, with the exception of CSIS. The amount of information shared is on a need to know basis in order for CSIS to conduct a full screening assessment as mandated by the PGS. For example, the RCMP is only provided with the individual's name, date of birth and address to support their HIPSSS queries. In addition, an arrangement was made between the RCMP and the CBSA, that the RCMP only provide us with specific types of information derived from the Law Enforcement Record Check that would only be pertinent to security screening. This will be detailed in the forthcoming MOU.

The RCMP databases queried as part of the Law Enforcement Record Checks (LERC) currently include: CPIC, ACIIS, NCDB, PROS, PIRS, PIP, PRIME, SCIS, SPROS, and Interpol. Databases can change and therefore, the preceding the list should not be considered all inclusive. Information found in these databases typically contains criminal charges and convictions, youth findings of guilt, and criminal intelligence.

It should be noted that the RCMP conducts these checks of relevant law enforcement files, including intelligence gathered for law enforcement purposes and provides the originating agency that holds this information with tombstone data (name, DOB, address) to support a request to release the information to the CBSA for a personnel security screening assessment. Information obtained through a LERC check will only be released to the CBSA by the RCMP with the approval of the originating police agency. This information will be disclosed to individuals applying for a security screening if the information is used in a review for cause investigation or when a decision is made to refuse or revoke a screening.

Equifax is also only provided with the name, date of birth and address to support their credit queries.

The CBSA will only retain personal information for the minimum amount of time necessary to ensure it is of no enduring value to the Agency.

It has been established that the minimum retention period for Records will be 2 years after an employee has left CBSA and then records are destroyed. If a security screening level is revoked, records will be retained for 5 years and then destroyed.

The CBSA received TB approval to implement the following assessment tools within the reliability status security screening process:

1. To utilize an Integrity Questionnaire, which has been discontinued. However, modified questions have been used to develop the Integrity Interview Guide which is in the conduct of Integrity interviews;
2. To conduct an integrity interview;
3. To query the CBSA enforcement databases with Customs and Immigration information;
4. To query the Royal Canadian Mounted Police (RCMP) databases for Law Enforcement Record Checks;
5. To query the Citizenship and Immigration Canada (CIC) enforcement databases, which has not been implemented;
6. To administer a psychological test to further assess ethical behaviour, integrity and honesty of candidates where required.

3. Risk Impact to the Institution Should the Information be Compromised: Reputation harm, embarrassment, loss of credibility.

Privacy Risk:

Should the agency not implement the enhanced screening initiatives, the risk posed to the agency's reputation will be high as there is currently an increase in employee fraud and corruption, some of which is publicized in the media, causing embarrassment to the agency and a loss of credibility. Should this problem of fraud and corruption not be mitigated, it will cause decreased confidence in the agency by the public, put elected officials under the spotlight in a negative way, prevent the agency from meeting its strategic outcome as well as meeting the goals set by the Government of Canada.

Risk Impact to the Individual or Employee Should the Information be Compromised: Reputation harm, embarrassment.

Privacy Risk:

The type of information that will be gathered deals with an individual's criminal history, customs or immigration violations, immigration history, driving history, alcohol/drug use, gambling, security issues, use of force, unlawful sexual activity, involvement with law enforcement, employment, involvement with computers or technology, lifestyle and psychological state. This information, if divulged, could have a negative effect on the individual's reputation and could cause embarrassment.

Mitigation:

1. The CBSA will ensure the disclosure of personal information collected for personnel security screening purposes will only be disclosed in accordance with the relevant legislation as indicated in this PIA.
2. Only authorized employees of the CBSA, as part of their official duties as security screening officers, will be provided access to personnel security screening information.
3. The CBSA will take steps to ensure that particularly sensitive personal information, such as an Integrity Interview results are only accessed and viewed by authorized employees who require access to support their official duties as a security screening official.

4. Communication products available to the public and to employees provide guidance on safeguarding personal information. For example, the Q&A's to support the Officer Induction Training program and a link to the PGS Policy is available to the public.
5. Employees of the CBSA are given mandatory training on Personnel Security Screening, Physical Security and IT Environment, Security Awareness E Learning module, ATIP, Breaches of Information, Credit Check, and Values and Ethics.
6. The CBSA Standard Operating Procedures and Policy to support security screening have detailed instructions how to safeguard personal information (Annex 3).
7. Employees of the Personnel Security Screening Section are security cleared at Secret or Top Secret Level and they are all provided with a detailed security briefing at the time they are employed as a personnel security screening official.
8. Access to personal information will be monitored by way of audits and quality control mechanisms integrated within the procedures.

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

The following annexes have been previously submitted to the OPC:

- Annex 1_Threat Risk Assessment (TRA) PerSec Room 9th Floor
- Annex 2_Agency Personnel Security Screening APSS SoS
- Annex 3_HIPSSS Standard Operating Procedures - ANNEX E
- Annex 4_Message to All SPSD staff regarding Access to the Personnel Security Screening file room
- Annex 5_Integrity Questionnaire
- Annex 6_IQ Justification Preamble
- Annex 7_IQ Justification chart
- Annex 8_Dr. Barker - EP537-060013 Contract
- Annex 9_IA Pro (PSCMS)- Service Level Agreement
- Annex 10_Agency Personnel Security Screening APSS TRA
- Annex 11_HIPSS Physical Security TRA Review
- Annex 12_Contract for Credit Check Services between the CBSA and Equifax
- Annex 13_RCMP Signed Letter of Intent
- Annex 14_Government of Canada Personnel Screening, Consent & Authorization - Form TBS 330-23
- Annex 15_Government of Canada Security Clearance Form TBS 330-60
- Annex 16_HIPSSS Process Flow
- Annex 17_OPC Privacy Risks
- Annex 18_OPC Privacy Four Part Test
- Annex 19_Nov.14 Letter from OPC
- Annex 20_PerSec Functional Management Model Reporting
- Annex 21_Employee Misconduct Risk Assessment
- Annex 22_Cases and studies that demonstrate significant risks for corruption, fraud and criminal interference in the CBSA
- Annex 23_FMM Reporting for Key PERSEC Activities
- Annex 24 - Original PIB TBS Registration
- Annex 25_HIPSSS Implementation Phases Nov 2012

Name of Program / Activity / Service

PIA

Annex 26 – Account of Changes between 1st and 2nd Integrity Questionnaires
 Annex 27_RTOC.pdf
 Annex 28_CIC Database check.doc (which has not been implemented)
 Annex 29_Open Source Internet Checks
 Annex 30_OPC Letter of Recommendations 2012-12-18
 Annex 31_Response letter to the OPC 2013-02-17
 Annex 32_Executive Summary of CBSA Responses to the Office of the Privacy Commissioner's Recommendations

The following annexes are new and have not been previously submitted to the OPC:

Annex 33 - Justification for the Questions in the Integrity Interview Guide
 Annex 34 - Integrity Interview Guide
 Annex 35 – The Response to the OPC's letter of July 30, 2013,
 Annex 36 – The Four-Part Test of R. v. Oakes for Necessity and Proportionality for the HIPSSS

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the core PIA as they relate to the administration of the identified program or activity.

 Claude Rochette
 Vice President
 Comptrollership Branch, CBSA

 Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.

 Dan Proulx
 Director - ATIP, CBSA

 Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks